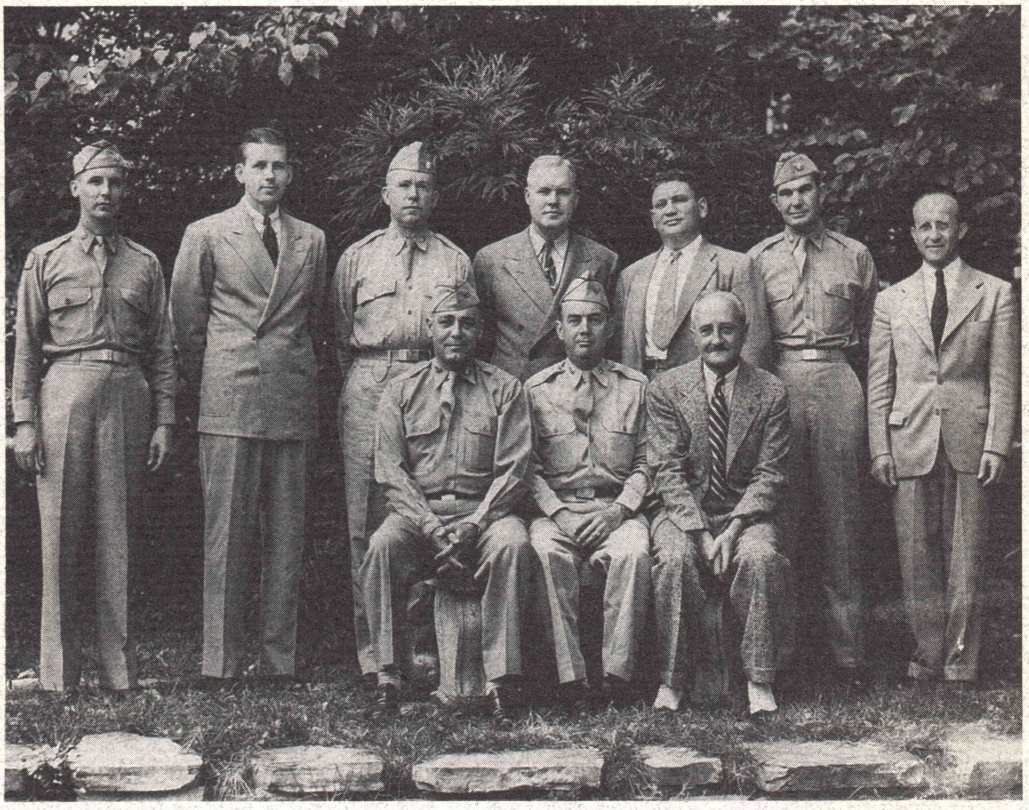
Volume XIX Number 2, April 1995

CRYPTOLOGIA

A QUARTERLY JOURNAL DEVOTED TO CRYPTOLOGY



CRYPTOLOGIA

A Quarterly Journal Devoted to Cryptology

All correspondence concerning subscriptions, advertising and publications should be sent to the publisher at the Editorial Office, Rose-Hulman Institute of Technology, Terre Haute IN 47803 USA. 812-877-8412. TELEX 752486.

[Cover: Army Security Agency Staff - 9 August 1946.

Seated from left to right: Colonel George A. Bicher, Colonel Harold G. Hayes, William F. Friedman.

Standing left to right: Hamill D. Jones, D. Glenn Starlin, James H. Frier, Jr., Frank B. Rowlett, Solomon Kullback, J. E, Wood, Abraham Sinkov.]

See inside back cover for subscription information and Call for Papers.

ISSN 0161 - 1194. Manufactured in the United States of America.

Assistance of Rose-Hulman Institute of Technology is acknowledged and appreciated.

WERE THE JAPANESE ARMY CODES SECURE?*

Edward J. Drea

ADDRESS: 10807 Ann St., Fairfax VA 22030 USA.

ABSTRACT: This essay describes various Imperial Japanese Army code and cipher systems used during World War II. Relying on Japanese and English language sources, it explains the multiple encryption methods employed by the Japanese to achieve radio communications' security. The article identifies specific characteristics of diverse Japanese code systems including the major army and army air force, water transport, military attache, air-ground, weather, and tactical systems. The narrative analyzes Allied cryptanalysts' accomplishments against these multiple Japanese systems and evaluates reasons for their success or failure. It concludes with an assessment of the overall effectiveness of the precautions taken by the Japanese Army to render its encoded military radio messages unreadable.

KEYWORDS: Army, ciphers, codes, communications' security, cryptanalysis, cryptology, discriminants, Japan, military, radio communications, World War II.

In 1984 an article titled "Nihon rikugun angō wa 'antai' datta" (The Japanese army's codes were secure!) appeared in a popular Japanese journal.[1] The author, former Imperial Army Major Kamaga Kazuo, had himself been a military cryptographer and cryptanalyst in Imperial General Headquarters during World War II. Kamaga's ringing defense of Japanese army codes was prompted by two earlier essays by Iwashima Hisao, then Chief, First Military History Division, National Institute for Defense Studies. Iwashima had asserted that far from having inviolable secrecy, Japan's military codes were easily and thoroughly read by the Allies.[2]

*I am indebted to David Kahn for his incisive comments and editorial assistance on an earlier version of this article. I am also grateful to Joseph E. Richard for his comments and for sharing with me his first-hand knowledge of Central Bureau operations.

[1]Kamaga Kazuo, "Nihon rikugun angō wa 'antai' datta," (The Japanese army codes were secure) *Rekishi to jimbutsu - zōkan: Shōgen - Taiheiyō sensō* (Rekishi to jimbutsu, special issue - Testimony - the Pacific war) (September, 1984), 270 - 282. Kamaga elaborated his thesis in two later articles. See Kamaga Kazuo, Fujiwara Kuniki, and Yoshimura Akira, "Zandankai: Nihon rikugun angō wa naze yaburarenakatta," (Discussion: Why couldn't the Japanese army's codes be broken?) *Rekishi to jimbutsu - Taiheiyō sensō shirizu:Nihon rikukaigun kaku tatakaeri* (Rekishi to jimbutsu, Pacific war series: The war between the Japanese army and navy) (December 1985), 150-165 and Kamaga Kazuo, "DaitōA sensō ni okeru angōsen to gendai no angō," (Code warfare in the greater East Asia war and today's codes) Dōdai kurabu koenshū, eds., *Shōwa gunji hiwa* (Secret tales of the military during the Showa emperor's reign) (Tokyo: Dōdai kurabu, 1989), 170-201.

[2]Iwashima Hisao, "Kazuresatta Nihon rikugun angō no 'shinwa'," (Crumbling away the myth of the Japanese

After an unusually harsh ad hominem dismissal of Iwashima's qualifications, Kamaga explained the cryptographic scheme that rendered major Japanese Army code systems unreadable by outsiders. While acknowledging that the capture of Japanese code books had enabled the Allies to decipher some messages in various code systems, Kamaga concluded that the army's codes were secure. He reasoned that sophisticated military cryptographic practices plus the great variety of Japanese army code systems safeguarded security.

Indeed, like other military forces, the Japanese did rely on great numbers and variations in their codes to guarantee that no outsider could read their secret messages. Sixty-three German Enigma key nets, for instance, were operational before the end of 1942, and during World War II the Imperial Japanese Navy had 24 naval systems current at any one time.[3] In neither case, however, did variety guarantee security. Nonetheless Kamaga's contentions are embedded in Japanese military cryptology during World War II, that is, how the Japanese army code systems worked. This essay examines those two pillars of cryptology and code multiplicity upon which Japanese military radio communications rested. My purpose is to determine whether or not Kamaga's argument has validity.

Japanese code security began in Japanese army communications' centers where cipher clerks prepared enciphered off-line messages. Imagine a second lieutenant striding down the drafty, narrow corridors of Imperial General Headquarters (IGHQ) in Tokyo. He turns into the General Affairs Section of the Army Department where he passes a hand-written message, stamped kimitsu (top secret), to a corporal code clerk perched behind a wire screen. The corporal had seen the red, square seal of the Army chief of staff too often to be much impressed. Still he quickly stamps a copy of the message and returns it to the young lieutenant as a receipt. The officer then leaves for the Army Operations Section to resume his uneventful night duty. Meanwhile the corporal passes the plaintext message to a private first-class who begins the monotonous task of encrypting the contents.[4]

---

army codes) Asahi jyānaru (September 4, 1981), 106-110 and "Rikugun angō antai shinwa no hōkai," (The collapse of the myth of secure army codes) *Rekishi to jimbutsu - zōkan: Shōgen-Taiheiyō sensō* (Rekishi to jimbutsu, special issue-testimony-the Pacific war) (August, 1983).

[3]See F. H. Hinsley, *et al.* eds., *British Intelligence in the Second World War: Its Influence on Strategy and Operations Volume Two* (London: Her Majesty's Stationary Office, 1981), Appendix 4, 658. Refer also to Alan J. Stripp, *Codebreaker in the Far East* (London: Frank Cass, 1989), 66 who notes 52 variant Enigma keys for the period between June 1943 and June 1944 - 21 army, 10 navy, 16 air force, and 5 for security services, SS, and police units. In the Japanese case, see Stripp, 65-66. More detailed information on Japanese naval codebooks is found in Military Intelligence Service Group, G-2, Headquarters, Army Forces Far East, trans., "Operational History of Japanese Naval Communications, December 1941-August 1945," reprinted and published by (Laguna Hills, CA: Aegean Park Press, 1985), 91-94.

[4]The description of IGHQ is adapted from "Kaiko: Ichigayadai," (Recollections of IGHQ at Ichigaya), *Zōkan: Rekishi to jimbutsu: Hiroku: Taiheiyō sensō*, (Special Issue: confidential: the Pacific war) (September

The Imperial Japanese Army employed a book-based, hand-written, cryptosystem. It used a two-part code. One part for encoding was arranged by Chinese ideographs or kanji and Japanese kana[5] according to the I, Ro, Ha system of the Japanese alphabet. The other part, for decoding, was arranged by digits in numerical order. Each contained 10,000 four-digit groups numbered from 0000 to 9999 which offered 9,500 meanings. The remaining 500 groups were intentionally left blank both as a security measure and as a way to insert new meanings into the codebook. The codebook was the initial step in encrypting a message.

The private first-class first encodes the plain text message word for word in the current Army General Purpose Code Book (Rikugun angōsho). For example, say the encoded form of hohei shidan (infantry division) is 1234. He encodes hohei shidan as 1234, then moves on to the next steps. The code clerk pulls out an additive book (ransūhyō). It contains a series of four-digit numbers arranged at random in a book of 100 pages, each containing 100 random four-digit numbers arranged in 10 columns and 10 rows. He then refers to the current regulations governing the additive. These give the clerk the page, column, and row of his first four-digit group. Next he fills in the first two boxes on his prescribed message form. The first four-digit group tells the code system in use, say 2345; the second indicates starting point in the additive, say 8145, or page 81, column 4, line 5. The code clerk receiving the enciphered message relies on these two four-digit groups preceding the actual message to tell him the code system in use (discriminator) and his starting point in the additive book (indicator).

Now the private begins to encipher the message text. To encipher hohei shidan, the clerk adds 1234 (code) to say 6789 (additive). Through noncarrying addition the enciphered version of hohei shidan becomes 8913. The enciphered version changed with each recurrence because the code clerk used a different additive group each time. In the case of hohei shidan, 1234 remains constant, but with the new additive, say 3456, its second appearance becomes 4680 thus confusing the codebreaker. This system alone is a fairly difficult cryptanalytic problem. Japanese cryptologists, however, employed other devilish complications to all their high-level four digit code systems.[6]

1982), 11-18, and the author's visit to Ichigaya in December 1985.

[5] Kana is the general term for the Japanese syllabic writing systems. Unlike kanji which express the meaning of individual words, kana express the 48 basic sounds plus 25 other sound changes of Japanese.

[6] Based on recently declassified documents, this is a revision and correction of my earlier explanation of Japanese army code systems which appeared in Edward J. Drea, *MacArthur's ULTRA: Codebreaking and the War Against Japan, 1942-1945* (Lawrence, KS: University of Kansas Press, 1992), 1-4.

↱	0	1	2	3	4	5	6	7	8	9
0	3	6	5	2	0	8	9	4	1	7
1	9	7	1	0	6	2	4	5	8	3
2	8	5	6	9	4	3	2	0	7	1
3	6	2	9	1	8	5	7	3	4	0
4	5	9	2	7	3	6	1	8	0	4
5	7	0	4	8	2	1	3	9	5	6
6	0	8	3	5	1	4	6	7	9	2
7	2	1	7	4	5	9	0	6	3	8
8	1	4	0	3	9	7	8	2	6	5
9	4	3	8	6	7	0	5	1	2	9

Figure 1a. Enciphering Conversion Square.

↱	0	1	2	3	4	5	6	7	8	9
0	6	5	8	1	0	9	7	2	4	3
1	8	7	1	3	6	5	4	9	0	2
2	7	3	4	0	5	1	2	8	9	6
3	0	9	6	8	4	2	5	3	7	1
4	9	8	5	7	2	6	1	0	3	4
5	4	2	0	6	7	3	9	1	5	8
6	3	0	2	9	1	4	6	7	8	5
7	5	1	7	4	9	8	3	6	2	0
8	2	6	9	5	3	0	8	4	1	7
9	1	4	3	2	8	7	0	5	6	9

Figure 1b. Deciphering Conversion Square.

Reproduced with the permission of Mr. Kanatomi Yoshiji, Dōdai kurabu.

They used 10-by-10 conversion or substitution squares (tokubetsu keisanhyō) (Figure 1a) for even greater security for their radio messages. Instead of adding the code number and the key number, they passed each of their digits through a conversion square. If the plain code number was 1234 and the key number 6789, the cipher clerk enciphered the 1 with the 6 by replacing the number 1 with the number that stood at the intersection of the row headed by 1 and the column headed by 6. In the square of Figure 1a, this is 4. For the entire codegroup, the cipher clerk arrived at the figure 4044 instead of 8913. A deciphering table (Figure 1b) facilitated deciphering. This system meant that a cryptanalyst, instead of merely knowing how to add, had to recover the square before reaching the key - before then discovering the plaintext.[7]

[7]Henry D. Ephron, "An American Cryptanalyst in Australia: Supplementary Comment from 'DENDAI' (Henry D Ephron)," *The Australian Rationalist Quarterly*, (Jan.-Feb.-Mar., 1982), 7; Kamaga Kazuo, "DaitōA sensō ni okeru angōsen to gendai angō," 177; Stripp, *Codebreaker in the Far East*, 91-92, describes a variant in which one read "into" a column-rank square as opposed to Kamaga's explanation of reading "around" the

To further obstruct would-be codebreakers, Japanese radio operators cut long Japanese four-digit military messages into sections of 50 groups each. They then scrambled the order of the message parts transmitting say a seven-part message in random sequence as part 7, 2, 6, 3, 1, 5, and 4. Each 50 group part contained a number of groups for identification purposes. The most important was the internal message number or dendai (electrical message number). This serial usually stood in the middle of the message because the final section was cut off at some arbitrary point and placed at the beginning.[8] The technique buried the discriminant and indicator somewhere within the multipart message instead of standing at the beginning as was more common. In brief the Japanese relied on a series of complicated encryption and transmission procedures for first-line security.

The Japanese army's major four-digit code systems also had yet another line of defense: regional or local ciphers. The entire theater of operations was divided into code areas. Major headquarters units used common four-digit code books, but different area army-level headquarters[9] used different conversion squares. Later, when cutoff from normal distribution, they resorted to a different conversion square specially established for their area. Higher headquarters designated the square and then transmitted the special square to all forces requiring it.[10] A four figure discriminant specified the particular codebook, additive book, and substitution square necessary to decrypt a high-level, four-digit message.

Thus the Japanese army employed a variety of book-based code systems. Each consisted of several components. The decrypted message (Figure 2)[11] lists the components required to decipher the Army Water Transport Code, known by its discriminant 2468.

Some representative main-line four-digit book systems are given below with discriminants indicating the additive or conversion table encipherments for the various code areas:

---

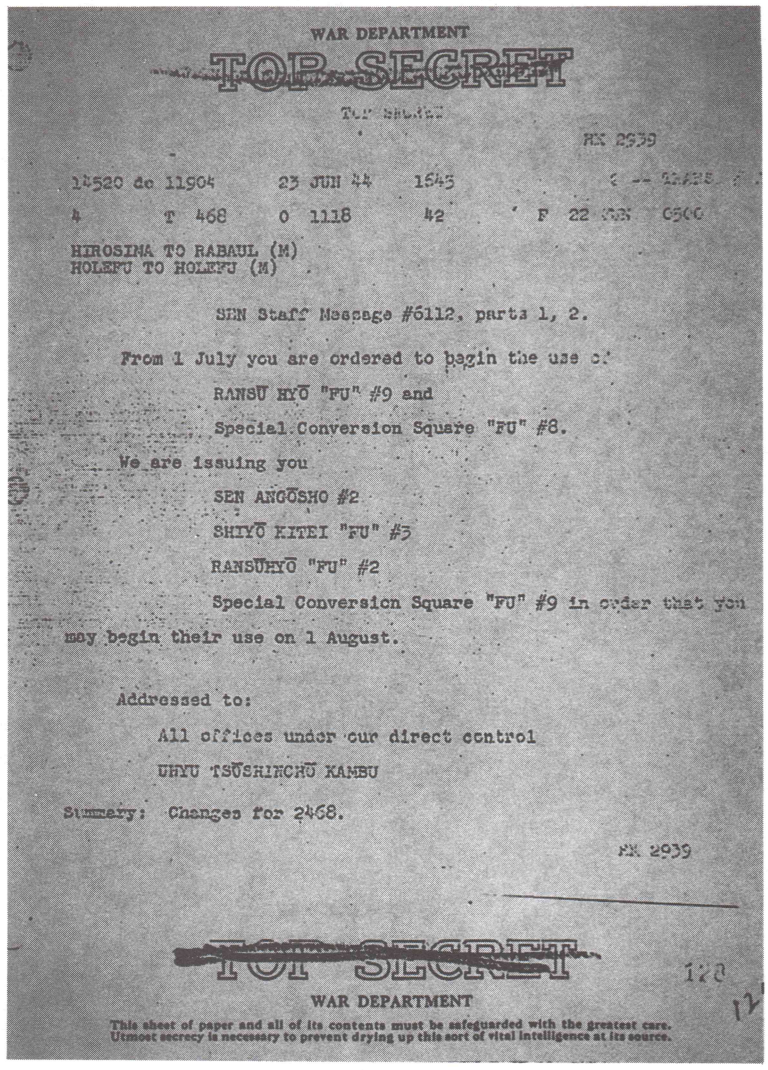
reverse conversion square. See also Alan Stripp, "Japanese Army Air Force codes at Bletchley Park and Delhi," in F. H. Hinsley and Alan Stripp, eds., *Codebreakers: The Inside Story of Bletchley Park* (New York: Oxford University Press, 1993), 296-299.

[8] Henry D. Ephron, "An American Cryptanalyst in Australia," *The Australian Rationalist Quarterly*, April-May-June, 1980. Reprint *Cryptologia* (October, 1985), 339-340.

[9] A Japanese area army consisted of two or more armies or the equivalent of an American army. A Japanese army consisted of two or more divisions or the equivalent of an American corps.

[10] For the Japanese navy's use of a similar technique see "Operational History of Japanese Naval Communications," 81-84.

[11] SRH-280, "An Exhibit of the Important Types of Intelligence Recovered through Reading Japanese Cryptograms, WW II," 124, Record Group 457, U.S. National Archives and Records Administration, Washington, D.C. Hereafter referred to as SRH-280. Unless otherwise noted all subsequently cited SRH documents are found in Record Group 457.



WAR DEPARTMENT

TOP SECRET

TOP SECRET

RX 2939

14520 do 11904 23 JUN 44 1543 [illegible]

4 T 468 0 1118 42 F 22 [illegible] 0500

HIROSIMA TO RABAUL (M)
HOLEFU TO HOLEFU (M)

SEN Staff Message #6112, parts 1, 2.

From 1 July you are ordered to begin the use of:

RANSŪ HYŌ "FU" #9 and

Special Conversion Square "FU" #8.

We are issuing you

SEN ANGŌSHO #2

SHIYŌ KITEI "FU" #3

RANSŪHYŌ "FU" #2

Special Conversion Square "FU" #9 in order that you may begin their use on 1 August.

Addressed to:

All offices under our direct control

UNYU TSŪSHINCHŌ KAMBU

Summary: Changes for 2468.

RX 2939

TOP SECRET

WAR DEPARTMENT

This sheet of paper and all of its contents must be safeguarded with the greatest care. Utmost secrecy is necessary to prevent drying up this sort of vital intelligence at its source.

Figure 2. The message, sent by unyu tsūshinchō kambu (transport signals' staff) explains the scheduled changes for July and August 1944 to the army code system identified by discriminant 2468. Sen angōsho #2 tells the code clerk to use *Senpaku angōsho* (Army Water Transport Code 2nd Edition) in conjunction with Shiyō kitei "Fu" #3 (Regulations governing the use of System "Fu" #3), Ransūhyō Fu #2 and Special Conversion Square Fu #9. Thus deciphering a message in the 2468 system for a two-month period in mid-1944 required the following components: the *Senpaku Angōsho* #2 (the four-digit Water Transport Code Book 2nd Edition), Ransūhyō Fu #2 (the four-digit Random Additive Book Fu), and Tokubetsu keisanhyō Fu #9 (Conversion Square Fu #9).

Discriminant	Japanese Name	English Translation and Code Area
2468	Senpaku angōsho	Water Transport Code
2345	Rikugun angōsho #4	Army General Purpose Code #4
7777	Rikugun angōsho #4	Army General Purpose Code #4 (Second Area Army in New Guinea Code Area)
6666	Rikugun angōsho #4	Army General Purpose Code #4 (Eighth Area Army in New Britain Code Area)
5555	Rikugun angōsho #4	Army General Purpose Code #4 (Southern Army in Malaya Code Area)
3366	Kōkū angōsho #3	Army Air Force General Purpose Code
9012	Kempei angōsho #1	Military Police General Purpose Code
4321	Tsūshin angōsho #2	Communications General Purpose Code (18th Army in New Guinea Code Area)
7654	Tsūshin angōsho #2	Communications General Purpose Code (Eighth Area Army in New Britain Code Area)
6543	Tsūshin angōsho #2	Communications General Purpose Code (Southern Army in Malaya Code Area)

Discriminant 7777 specified the components needed to decrypt messages in the Army General Purpose Code Book originated by Second Area Army in western New Guinea and 6666 those of Eighth Area Army at Rabaul; discriminant 6543 specified the components of the Communications General Purpose Code used by Southern Expeditionary Army then headquartered in Singapore, and so forth. The Water Transport System (2468) had five code areas that equated to the five regional shipping transport headquarters at Hiroshima, Shanghai, Singapore, Rabaul, and Davao (in the Philippines) respectively.[12] In other words, different Japanese army major commands employed different cipher keys to further perplex putative codebreakers.

To return to the Imperial General Headquarters' message center, after his corporal nods perfunctory approval of the encryption, the private first-class bows, buttons his tunic, and takes the encrypted message to the Signal Message Center. He descends a staircase with its ponderous balustrades into the damp, musty

[12]The table is derived from Sanbō honbu (Headquarters general staff), "Rikugun angō ichiranhyō" (Table of army codes) Shōwa 20 nen kugatsu hatsuka (September 20, 1945) and S. Kullback, "Japanese Military Cryptographic Systems," 23 November 1943. Copies in possession of author.

basement of the three-story concrete building. Arriving at the message center, he hands the encrypted text to the communications officer on duty that night. The lieutenant logs in yet another of the 500 or so messages transmitted every day from IGHQ to Japan's far-flung armies.[13]

Administrative procedures completed, the lieutenant orders a sergeant nearby to take the message to the radio room. The sergeant walks into the even danker, cigarette-smoke filled recesses of an underground bombshelter. He stops at one of the several recesses cut into the arch-shaped bomb tunnel and hands the message to a radio operator. The radioman disguises the plaintext address prefixed to the message by a series of encodings. For this step he uses yet another set of code books, the unit address code and the geographic place name lists. He then logs in the message assigning it a file date and time, e.g., 12070700 for December 7, 0700. Finally he encodes the dendai or serial number of the message, its place of origin, and its place of destination.[14]

At last the enciphered message is ready for transmission over a Japanese military frequency to its destination. The Japanese military communications network was highly centralized. Each of 16 powerful signal centers beamed four-digit encrypted messages - either relayed from other commands or originated in their own - in army, army air force, army water transport, and army communications systems to subordinate headquarters throughout Asia and the Pacific.[15]

All significant messages passed through these nodes. Some messages were re-encrypted for dispatch to different code areas, despite the danger of this procedure.

After routine radio transmissions to test readability and signal strength, the Tokyo operator taps out his message manually, using the abbreviated Morse numerals. He transmits the message text enciphered as 2345 (discriminant), 8415 (indicator), and 8913 (hohei shidan) as "ZSMA WMNA WVNS." The receiving Japanese radioman in, say, the Singapore signal center, copies the numbers on his prescribed message form. He then breaks out the encoded address and delivers the cipher message to a code clerk of the appropriate, say, Second Army unit. He removes the conversion square encipherment of system 2345 and next reapplies the encipherment using the 7777 conversion square appropriate for that key net. Then, a radio operator of the Second Army unit of the cipher center transmits the message to Second Army in his next regularly scheduled broadcast. The

[13] Kamaga, "Nihon rikugun angō wa 'antai' datta," 281 estimates 500 messages transmitted daily.

[14] Henry D. Ephron, "An American Cryptanalyst in Australia," 340 and SRH-362 "History of the Signal Security Agency, vol. 3, The Japanese Army Problem: Cryptanalysis, 1942-1945," 021.

[15] Nakamura Fumio, "Gunji tsūshinshi hanashi: Daihon'ei to tsūshin," (Stories about the history of military communications: Imperial general headquarters and communications) *Denpu to Juken* (September 1982), 108.

number of code systems coupled with the complex procedures used to prepare and transmit messages seemed to guarantee security of message contents.

Without access to all the components, the Japanese believed an outsider could not read the enciphered message, at least not in a timely fashion. The Japanese understood that their code books, key registers, and conversion squares might fall into enemy hands. It was the duty of the signals' officer both to destroy code material in danger of capture and to inform Tokyo of the destruction. Lacking such confirmation, Tokyo would assume its codes were compromised. Tokyo also realized that a solution might be possible if the enemy gathered a sufficient quantity of intercepted messages and devoted extensive time and resources to break the cipher. Naturally by that time the derived intelligence value would be nugatory or so the Japanese thought.

Nevertheless to preclude any solution, the Japanese routinely changed their conversion squares and somewhat less frequently the additive book. They also replaced most of their major four-digit code books at least once during the Pacific War (1941-1945).[16] Besides shifting the components of a cryptosystem, each change of conversion squares introduced a whole new mathematics to befuddle the enemy cryptanalyst. In short, possession of a Japanese codebook alone did not automatically enable Allied cryptanalysts to break Japanese military ciphers. Procedurally, then, an ever-changing code system gave the Japanese confidence that, with only some of the components, the Allies could not read their plaintexts.

The other source of Japanese confidence in their communications security was the variety of Japanese code systems. These ranged from the diverse high-level Japanese major four-digit ciphers through the tactical three-digit unit substitution table cipher to lower level three-kana naval land-based air or weather transposition codes.[17]

Rikugun angōsho 3 (army general purpose code 3d edition), the most important four-digit Army cipher, was current on December 7, 1941, and remained in effect until edition No. 4 was introduced June 1, 1943; No. 5 was introduced 1 January 1945. Rikugun angōsho was the general-purpose code for ground forces distributed to all Japanese army units from independent brigade through area army including those in the Central Pacific, Solomons, and New Guinea as well as Imperial General Headquarters in Tokyo. Its additive book changed every three to six months and its special conversion square changed every few weeks. Edition No. 5 was distributed to all Japanese army units except those cutoff on New Britain and New Guinea. Its key register changed at four month intervals and its conversion square changed every one to three weeks.

[16] See Appendix for a partial list of Japanese codes.

[17] "Rikugun angō ichiranhyō."

The U.S. Army's Signal Intelligence Service (SIS) at Arlington Hall Station, Virginia, first broke into Code Book No. 4 in September 1943, but the Australians' capture of the Japanese 20th Infantry Division's cryptographic library at Sio, Northeast New Guinea, in January 1944 fully bared the system's secrets. Central Bureau, General Douglas MacArthur's independent cryptanalytic center then located at Brisbane, Australia, and Arlington Hall read this code with some interruptions from January 1944 onwards.[18] On August 1, 1944, the Japanese army began enciphering discriminants with a special additive book.[19] Fortunately for the Allies by that time it was possible to identify and separate the main systems even without knowing the discriminants. Moreover cryptanalysts soon recovered the separate additive book so that a continuous solution was possible until January 1945 when Rikugun angōsho 5 appeared. Code books captured in the Philippines and Okinawa enabled the Allies to begin reading edition No. 5 with regularity by June 1945.[20]

The Japanese army air force's main system (3366)[21] also was a four-digit code, kōkū angōsho No. 2 (air force general purpose code 2nd edition), in effect December 1941. It underwent two changes during the war, one around March 1943 and the second on 1 February 1945. It relied on an additive table with a three month life expectancy and a monthly special conversion table for messages of army air force ground units. Its purpose was to conceal top-level communications between Imperial General Headquarters and air division and higher echelons. Subordinate commands employed a subsystem of the main one using a different monthly conversion table. The British Wireless Experimentation Center (WEC) Delhi, India, and the Government Code and Cipher School (GC&CS), Bletchley Park, Great Britain, seem to have been in the forefront of the cryptanalytic assault on this system. Arlington Hall did not devote considerable attention to these air systems until late 1944, although Central Bureau solved with regularity messages from the major Japanese air headquarters on New Guinea – Fourth Air Army as well as Sixth and Seventh Air Divisions using recoveries forwarded from Arlington Hall, GC&CS, and WEC.[22]

---

[18] On the Sio material see Drea, 92-93. SIS underwent several name changes during the course of World War II before ending up as SSA or Signal Security Agency. I have used Arlington Hall throughout this paper as synonymous with SIS and its successors.

[19] SRH-362, 106.

[20] "Message LTC A. W. Sanford, G.S. to C-in-C, A.M.F.," 30th June 1945, Papers of Field Marshall Sir Thomas Blamey World War, 1914-1918, 1939-1945, Australian War Memorial (Canberra) (AWM), File 2/56.

[21] Stripp, *Codebreaker in the Far East*, 77-78 and Chapter 9 *passim* as well as his "Japanese Army Air Forces codes at Bletchley Park and Delhi," describes the 3366 system.

[22] SRH-059, Selected Examples of Commendations and Related Correspondence Highlighting the Achievements of U.S. Signal Intelligence during World War II, 031. SRH-349, 029. See also Stripp, "Japanese Army

Unquestionably by the end of June 1945, Central Bureau was reading traffic encrypted in the army air force main system destined for commands in China, Korea, Manchukuo, and the Southern Region.[23] A variant of 3366 was system 6633, the same four-digit reciphered code with a different conversion square. The Japanese used 6633 extensively in Burma.[24] Apparently GC&CS at Bletchley Park also broke these systems sometime in 1943.

Air force garrisons exchanged administrative messages via the kōkū hoan angōsho No. 1 (air maintenance code 1st edition, discriminant 3636), effective December 1941, superseded on February 1, 1945. Its security depended in part on an additive table that changed quarterly. Army air force and antiaircraft units used it for internal communications to air force units, air force headquarters, and air ground communications. Messages in 3636 reported conditions of runways, fuel supplies, and weather.[25] The Allies were aware of this system but open sources do not reveal to what degree, if any, they were able to read it.

The Japanese army also had an extensive transport fleet whose command and control authorities used the senpaku angōsho (water transport code, discriminant 2468). A first edition was current in December 1941; the 3d appeared on 1 June 1945. This was a four-digit cipher distributed to water transport units along with an additive book that changed every three or four months and a conversion table that changed every three weeks. It shared many cryptographic similarities with the main army cipher, but had separate code and additive books as well as conversion squares. Message traffic in the 2468 system appeared in volume around December 1942, coinciding with the large scale movement of Imperial Japanese Army units to the Bismarck and Solomon Islands and to New Guinea. Both Central Bureau and Arlington Hall Station broke this code system, the first high-level system they decrypted, almost simultaneously in April 1943. The Allies read 2468 without interruption until the codebook changed in June 1945.[26] By that time the volume of Japanese water transport messages was so low and so fragmented into several systems using different conversion squares that solution was slow.

Other four-digit book codes were the tsūshin angōsho 2 (communications code 2nd edition) in effect December 1941 until replaced by No. 3 effective on October

Air Forces codes at Bletchley Park and Delhi," 284, 296-299.

[23] Message Sanford. The so-called Southern Region included Burma, Malaya, Netherlands East Indies, New Guinea, and Philippines.

[24] Stripp, *Codebreaker*, 77-78.

[25] "Rikugun angō ichiranhyō," and Kullback, "Japanese Military Cryptographic Systems."

[26] Drea, 74-75 and author's interview with Mr. Joseph E. Richard, Silver Spring, Maryland, March 5, 1993. Mr. Richard served as a cryptanalyst at Central Bureau and was awarded a Legion of Merit for his work against the water transport and other Japanese cryptographic systems.

1, 1944. Japanese signal centers and ground communications units employed this system to pass information pertinent to changes of call signs, radio station location codes, address codes, and so forth. Messages explained how to handle radio traffic and assigned call signs and radio frequencies. In the case of signal center code books, the tsūshin angōsho also gave dates of forthcoming cryptographic changes, explained the methods of constructing and applying the keys (shiyō kitei), and the meanings of code groups, as well as designating the particular edition in use.[27] Because their duties were administrative, signal center radiomen could read addresses and discriminants in order to sort message traffic, but they had no responsibility for and indeed could not decrypt the text of the message. In such circumstances, Allied ability to read the Japanese army's tsūshin angōsho sometimes enabled Allied codebreakers to anticipate alterations and revisions to the enemy cryptologic systems although the actual changes to major, four-digit systems were usually sent in the system being altered and not in a communications code.

The communication codebook's additive key had a four month life and the conversion square a monthly one. Apparently Arlington Hall and WEC both solved this system. A variant codebook, the tsūshin butai angōsho (unit communications code), was distributed to brigade communications' units for headquarters' use. Its additive book changed either monthly or bimonthly.

Code clerks sorted all incoming messages according to the atena angōsho (unit address code) found in the message header. Edition No. 3 was current at the time of the Pearl Harbor attack and the unit address code underwent two changes during the war with No. 5 appearing 1 August 1945. Each Japanese army unit had a code name and number – e. g., Anchorage Unit 45 was Akatsuki 6433 – and this four-digit code disguised these ground and air unit addresses. Although sent in four-digit groups, the address code was actually a three-digit system as the fourth digit checked the first three.[28] The address code relied on an additive book of four months' duration and a special conversion table altered monthly or bimonthly.

Message preambles also included an encoded but not enciphered geographic place name. It gave the place of origin and the destination of the radiogram. The geographic place name code in use in 1939 remained effective until June 1942, when Tokyo distributed a new version to those units using the Army General Purpose Code. The geographic place name code had no additive or conversion table to disguise its codegroups. A new edition was issued April 1, 1945. WEC and SIS solved the geographic place name code in September 1942 and the unit

[27] SRH-280, 2.

[28] Stripp, *Codebreaker*, 71.

address code in 1943.[29]

The Japanese military police had their own cipher, the kempei angōsho (military police code, discriminant 9012). Version No. 2 was in effect in December 1941. Its replacement edition, No. 3, appeared on July 1, 1943. As the name implied, the kempei angōsho was used for communications between military police units and it was distributed to military police detachment and higher headquarters. The key register changed every four months and its conversion table monthly. This system, however, may have been peculiar to the Philippines under Japanese occupation.

Of two other high level systems – military attache and foreign ministry – only the former could in any way be regarded as a military system. Arlington Hall's Section III (General Cryptanalytic Problem) worked on their solutions. The bukanyō kanjihyō (military attache conversion table) was a two-letter substitution for common words, e.g., NW for ron (discussion). This was followed by a columnar transposition. It has been asserted that British cryptanalysts at Bletchley Park in the summer of 1942 were largely responsible for its solution. Declassified U.S. documents, however, suggest that the first break into the military attache code occurred in September 1942 and that Arlington Hall was reading the system from July 1943 with ease and regularity through March, 1945.[30]

Finally Arlington Hall became responsible for working the PURPLE machine, which of course generated MAGIC, or solved Japanese M-5 (or B-machine) diplomatic messages. U.S. Army and Navy cryptanalysts originally solved PURPLE in September 1940 but following a June 1942 agreement the Army did all the work on the system which was read throughout the war with Japan. Besides the PURPLE system, Arlington Hall also worked numerous other Japanese diplomatic codes, including a joint code of the Foreign Ministry and the Greater East Asia Ministry, Japanese agent codes, and so forth.[31]

The main tactical code of the Imperial Army was the butai kanjihyō 2 (unit substitution tables 2nd edition). It was in use in December 1941 and for all practical purposes served throughout the war, a third edition being introduced on August 1, 1945. Each Japanese division possessed a different field code so there were as many books as there were divisions, 101 in July 1944 and 179 by July 1945.[32] This three-digit code served for regimental liaison with subordinate units.

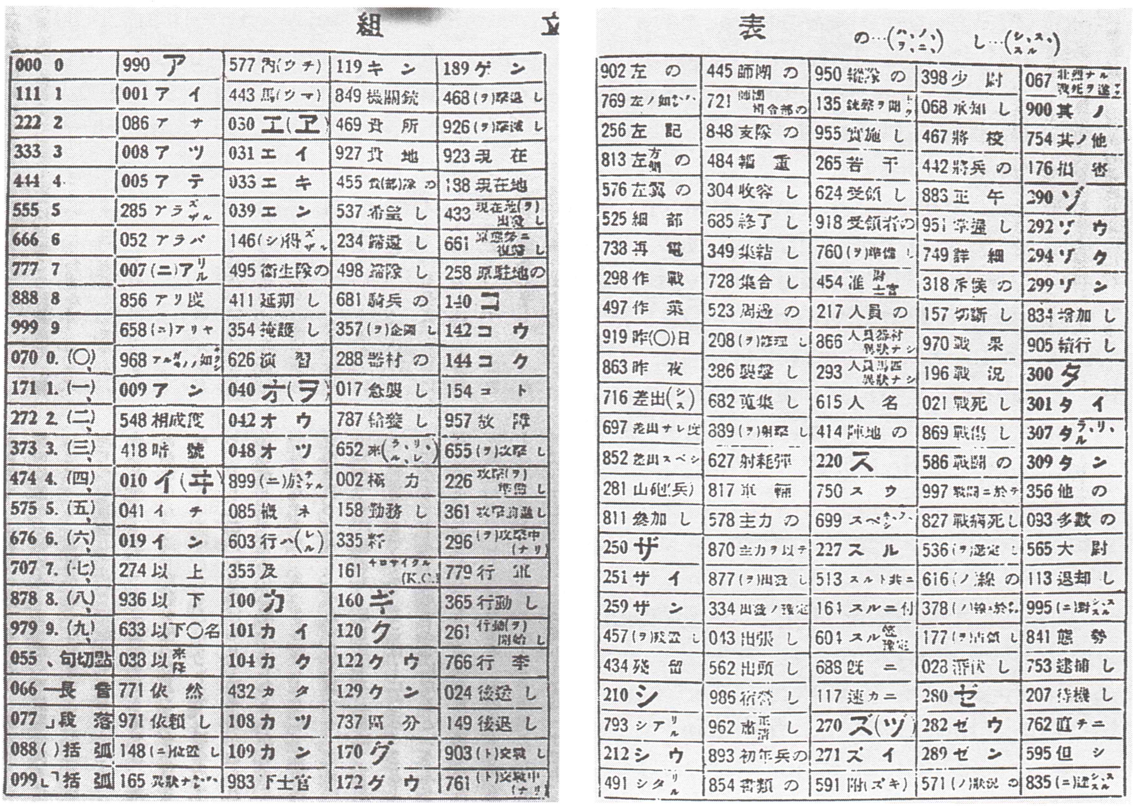
---

[29] Drea, 38.

[30] SRH-280, 12. Stripp, *Codebreaker*, 72 -73 and "Japanese Army Air Forces codes at Bletchley Park and Delhi," 283-4.

[31] SRH-355, "Naval Security Group History to World War II, " 090E. SRH-280, 013-018.

[32] S. Kullback, "Japanese Military Cryptographic Systems." My totals of Japanese divisions include four



組 立

000 0	990 ア	577 内(ウチ)	119 キ ン	189 ゲ ン
111 1	001 ア イ	443 馬(ウマ)	849 機關銃	468 (ヲ)撃退 し
222 2	086 ア サ	030 エ(ヱ)	469 役 所	926 (ヲ)撃滅 し
333 3	008 ア ツ	031 エ イ	927 我 地	923 現 在
444 4	005 ア テ	033 エ キ	455 我(部)隊 の	138 現在地
555 5	285 アラズザル	039 エ ン	537 希望 し	433 現在地(ヲ)出發 し
666 6	052 アラバ	146 (シ)得ズザル	234 歸還 し	661 原態勢ニ復歸 し
777 7	007 (ニ)アリル	495 衛生隊の	498 歸隊 し	258 原駐地の
888 8	856 アリ度	411 延期 し	681 騎兵 の	140 コ
999 9	658 (ニ)アリヤ	354 掩護 し	357 (ヲ)企圖 し	142 コ ウ
070 0. (〇)	968 アルモ,,如シ	626 演 習	288 器材 の	144 コ ク
171 1. (一)	009 ア ン	040 オ(ヲ)	017 急襲 し	154 コ ト
272 2. (二)	548 相成度	042 オ ウ	787 給養 し	957 故 障
373 3. (三)	418 暗 號	048 オ ツ	652 来(ラ、リ、ル、レ)	655 (ヲ)攻撃 し
474 4. (四)	010 イ(ヰ)	899 (ニ)於テケル	002 極 力	226 攻撃(ヲ)準備 し
575 5. (五)	041 イ チ	085 概 ネ	158 勤務 し	361 攻撃前進 し
676 6. (六)	019 イ ン	603 行ヘ(レ、ル)	335 軒	296 (ヲ)攻撃中(ナリ)
707 7. (七)	274 以 上	355 及	161 キロサイクル(K.C.)	779 行 軍
878 8. (八)	936 以 下	100 カ	160 ギ	365 行動 し
979 9. (九)	633 以下〇名	101 カ イ	120 ク	261 行動(ヲ)開始 し
055 、句切點	038 以來降	104 カ ク	122 ク ウ	766 行 李
066 ー長 音	771 依 然	432 カ タ	129 ク ン	024 後送 し
077 」段 落	971 依賴 し	108 カ ツ	737 區 分	149 後退 し
088 ( )括 弧	148 (ニ)位置 し	109 カ ン	170 グ	903 (ト)交戰 し
099 ㇄⌝括 弧	165 異狀ナシ	983 下士官	172 グ ウ	761 (ト)交戰中(ナリ)

表　の…(ハ、ノ、ヲ、ニ、)　し…(シ、ス、スル)

902 左 の	445 師團 の	950 縱隊 の	398 少 尉	067 壯烈ナル戰死ヲ遂ゲ
769 左ノ如シ	721 師團司令部の	135 銃聲ヲ聞ク	068 承知 し	900 其 ノ
256 左 記	848 支隊 の	955 實施 し	467 將 校	754 其ノ他
813 左方側 の	484 輜 重	265 若 干	442 將兵 の	176 損 害
576 左翼 の	304 收容 し	624 受領 し	883 正 午	290 ゾ
525 細 部	685 終了 し	918 受領者の	951 掌握 し	292 ゾ ウ
738 再 電	349 集結 し	760 (ヲ)準備 し	749 詳 細	294 ゾ ク
298 作 戰	728 集合 し	454 准尉士官	318 斥候 の	299 ゾ ン
497 作 業	523 周邊 の	217 人員 の	157 切斷 し	834 増加 し
919 昨(〇)日	208 (ヲ)修理 し	866 人員器材異狀ナシ	970 戰 果	905 續行 し
863 昨 夜	386 襲撃 し	293 人員馬匹異狀ナシ	196 戰 況	300 タ
716 差出(シ、ス)	682 蒐集 し	615 人 名	021 戰死 し	301 タ イ
697 差出サレ度	889 (ヲ)射撃 し	414 陣地 の	869 戰傷 し	307 タ ラ、リ、ル
852 差出スベシ	627 射耗彈	220 ス	586 戰闘 の	309 タ ン
281 山砲(兵)	817 車 輛	750 ス ウ	997 戰闘ニ於テ	356 他 の
811 參加 し	578 主力 の	699 スベキ、ク、シ	827 戰病死 し	093 多數 の
250 ザ	870 主力ヲ以テ	227 ス ル	536 (ヲ)選定 し	565 大 尉
251 ザ イ	877 (ヲ)出發 し	513 スルト共ニ	616 (ノ)線 の	113 退却 し
259 ザ ン	334 出發ノ豫定	164 スルニ付	378 (ノ)線ニ於ケル	995 (ニ)對シ、ス、スル
457 (ヲ)殘置 し	043 出張 し	604 スル豫定	177 (ヲ)占領 し	841 態 勢
434 殘 留	562 出頭 し	688 既 ニ	028 潜伏 し	753 逮捕 し
210 シ	986 宿營 し	117 速カニ	280 ゼ	207 待機 し
793 シアリル	962 掃蕩 し	270 ズ(ヅ)	282 ゼ ウ	762 直チニ
212 シ ウ	893 初年兵の	271 ズ イ	289 ゼ ン	595 但 シ
491 シタリル	854 書類 の	591 附(ズキ)	571 (ノ)狀況 の	835 (ニ)達シ、ス、スル

Figure 3. Two pages of the Butai kanjihyō 2 go or Unit Substitution Tables, 2nd Edition. The horizontal line across the top reads Kumitateruhyō or Organization Page. The numerals in the columns (except for the first ten) were randomly matched with words or phrases. The kanji (Chinese characters) and katakana (Japanese syllabary) are arranged according to the I, RO, HA system of the Japanese alphabet. Thus 445 (the top of the seventh column) is shidan (division), 848 is shitai (detachment), 349 is shūketsu (to assemble), to 854 shorui no (miscellaneous papers).

It relied on pads of randomly arranged numbers (mugen ransū) for encryption, strict radio operator security, low-powered transmissions, and vertical radio nets to achieve security. Apparently it was never compromised by the Allies.[33] Figure 3 shows a page from a three-digit book.

The sender's code book was organized functionally by subject. To encrypt a message, the regimental code clerk started with this book. After encoding each name or term separately, he enciphered the message, in this case by adding randomly arranged numbers selected from a pad.

Figure 4 shows a typical Japanese three-digit encryption on a message form showing Japanese plaintext, its encoding, the additive key, and the sum, which constitutes the cryptogram ready for transmission. The message reads in Japanese:

> Dai 3 daitai denpō 173 gō – Daitai wa jūji sanjūpun goro Tōzan ni oite heiryoku fumei no teki to sōgūshi, mokka kōsenchu nari.

Translation: 3d Battalion Signal No. 173 – About 10:30 A.M. near Eastern Mountain, the battalion encountered an enemy force of unknown strength. We are heavily engaged.

The top boxes of the standard message form are administrative – addresses, date-time group, originator, and so forth - the externals of the message. In this case they are blank, as lower-echelon units did not need the geographic place name code or unit address code. As often as not they dispatched messages to their headquarters without any external information. The rigid vertical structure of divisional signals' networks made this unnecessary. For example, the 66th Infantry Regiment, 51st Infantry Division, could only send messages upward to division headquarters and receive messages downward only from division level. It could not communicate horizontally to its two sister regiments. In brief the vertical network made unit identification somewhat superfluous.

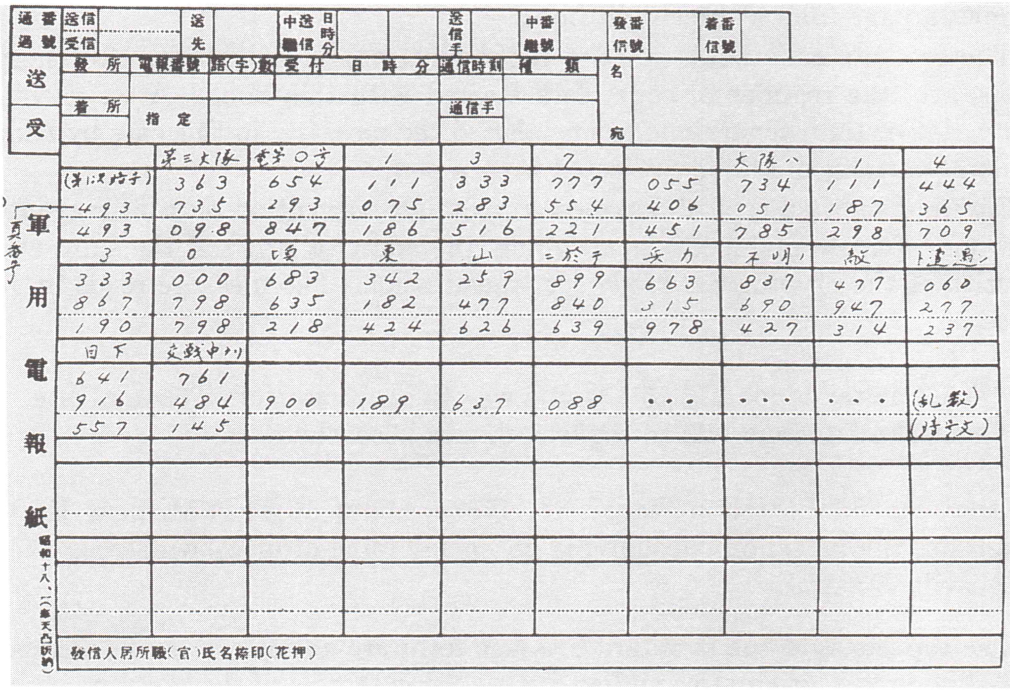
The next series of blocks contain the message itself. The first block, 493, is the discriminant. It tells the receiver from which number on a pad to begin when decrypting the message. The following block has three sets of numbers; 363, 735,

---

armored divisions in the July 1944 figures and four anti-aircraft artillery divisions in the July 1945 ones. All others were infantry divisions. I have not included air divisions in the totals because they used different field codes.

[33] Australian documents state that a three-digit divisional code book was captured (perhaps part of the 20th Division cache taken at Sio in January 1944) which enabled Central Bureau to read the 20th Division's three-digit communications for some time. See "Central Bureau Technical Records, Part J - Field Sections," n.p., Part II., para 2., Australian Archives (Victoria): Central Bureau, CRS B5436/1, Technical Records 1945-1946, Item No. IT J, 28. Hereafter cited as CBTR, J.

and 098. 363 is the encoded form of Dai 3 daitai (3rd Battalion). The additive from the pad is 735.



	第三大隊	武宇〇守	1	3	7		大阪八	1	4
(第1只拈子)	3 6 3	6 5 4	1 1 1	3 3 3	7 7 7	0 5 5	7 3 4	1 1 1	4 4 4
4 9 3	7 3 5	2 9 3	0 7 5	2 8 3	5 5 4	4 0 6	0 5 1	1 8 7	3 6 5
4 9 3	0 9 8	8 4 7	1 8 6	5 1 6	2 2 1	4 5 1	7 8 5	2 9 8	7 0 9
3	0	以東	東	山	二於テ	兵力	不明ノ	敵	上通過ノ
3 3 3	0 0 0	6 8 3	3 4 2	2 5 7	8 9 9	6 6 3	8 3 7	4 7 7	0 6 0
8 6 7	7 9 8	6 3 5	1 8 2	4 7 7	8 4 0	3 1 5	6 9 0	9 4 7	2 7 7
1 9 0	7 9 8	2 1 8	4 2 4	6 2 6	6 3 9	9 7 8	4 2 7	3 1 4	2 3 7
旧下	定数中ノ								
6 4 1	7 6 1								
9 1 6	4 8 4	9 0 0	1 8 9	6 3 7	0 8 8	・・・	・・・	・・・	(乱数)
5 5 7	1 4 5								(特字文)

Figure 4. A three-digit encrypted message form. The first block (493) is the discriminant. It tells the receiving code clerk from which number in the key register to begin his encipherment. Otherwise each vertical block contains four items. The top line is plaintext. The next line is the encoded version of the plaintext. The third line is the key register additive. The last line is the sum of lines two and three by means of false addition. The Dai 3 datai (3rd Battalion) encoded becomes 363. It is encrypted by adding it to 735 using non-carrying addition and becomes 098. The radio operator transmitted 098 in Morse Code as OVW.

In their spare time code clerks filled in the blocks containing additive numbers in red ink so the form usually was ready whenever the unit had to transmit a message.[34] By means of false addition, the sum 098 is the encrypted form of Dai 3 daitai. American cryptanalysts studied the three-digit army system until they determined in March 1943 that it was unreadable since it was based on a pad. They then shifted their cryptanalytic attack to the main four-digit Japanese army systems.

[34] Kamaga, "DaitōA sensō ni okeru angōsen to gendai no angō," 173.

Other Japanese tactical communications normally used three-digit or three-kana systems. For air-ground communications, the army air force used a series of three-digit books, the kū-chi renraku (air-ground liaison code). As a numerical code, operators sent it in International Morse Code. Obviously, it was used for air ground communications, but it was also employed by air headquarters' echelons and air units for communication among them. Edition No. 1 was issued 10 July 1941 and was in effect in December 1941. A copy of this codebook was captured at Singapore in January 1942.[35] The Allies captured subsequent versions during the course of the war.

In the early days of the Pacific War the air-ground code was not enciphered. Indeed, Allied intercept sites frequently caught their first indication of an impending air raid by overhearing a tactical air base headquarters warming up its radio strike frequency.[36] Later, however, the Japanese enciphered the code with a 1,000 group additive table that changed daily, the army hikōbutai kanjihyō (air unit substitution tables). Edition No. 1 was a three-figure code book in effect until superseded by No. 2 on 1 August 1944. A third change occurred in January 1945.[37] Allied cryptanalysts had to recover this 100 line table of 10 groups each daily. They usually accomplished this by intercepting and decoding routine weather reports.

Army air ground systems became important as army air units entered the fighting in the Southwest Pacific Area in late 1942 and early 1943. A codebook captured in India and one taken from a Japanese army bomber shot down over Bataan in early 1942 were the cribs into the system.[38] These captures allowed a continuous solution of Japanese army air force air-ground codes because the system remained essentially unchanged throughout the entire war. Field intercept sites often solved these simple code systems locally. When one understands that the kū-chi renraku systems transmitted weather reports, references to units, sightings, battle results, airfield conditions, and the like, one grasps its value to Allied codebreakers. [39] Japanese naval air-ground procedures, conversely, never

[35] "Central Bureau Technical Records, Part C - Army Air-Ground Communications," 7, Australian Archives (Victoria): Central Bureau, CRS B5436/1, Technical Records 1945-1946, Item No. IT C, 49. Hereafter cited as CBTR, C.

[36] CBTR, J, 26.

[37] CBTR, C, 7. This information matches that in "Rikugun angō ichiranhyō."

[38] "Central Bureau Technical Records, Part A - Organisation," 1, Australian Archives (Victoria): Central Bureau, CRS B5436/1, Technical Records 1945-1946, Item No. IT A., 5. Hereafter cited as CBTR, A. SRH-045, "Reminiscences of LTC Howard W. Brown," 4 August 1945, 031-032. Jack Finnegan, "Grim Fate for Station 6," *Military History*, (October 1986), 63 and General Headquarters, Far East Command, Military Intelligence Section, General Staff, "A Brief History of the G-2 Section, GHQ, SWPA, and Affiliated Units," Introduction, Intelligence Series, 1948, 6.

[39] CBTR, C, 1.

permitted names of units or information about aircraft availability to be passed in such a manner.[40] But the naval air force had its own problems with communications' security.

In addition to the three and four-digit codes, Japanese army air force aircrew used kana symbols – not numerals – to communicate with their bases about more routine matters like destinations, points of departure, landing instructions, estimated times of arrival or departure and so forth. Radio operators dispatched such messages in the Japanese kana Morse Code. Bases and aircraft used three-kana call signs, e.g. HA RU NA, and further separated call signs and radio frequencies according to transport and operational commands. Call signs for operational units changed about every 10 days but base call signs remained constant much longer.[41] For greater security, the army air force relied on the air-ground liaison code. But the systems failed to keep their secrets.

Various army-navy liaison codes such as the kyōdō sakusen angōsho 3 (joint operations code 3d edition) in use during December 1941 through No. 5, introduced April 1, 1945, depended on an additive book that changed monthly. A lower-grade version was the kyōdō chimei jiten (joint place name code) introduced late in the war together with the 5th edition. Unlike No. 5, however, it had no additive. Both systems were used by units involved in joint army-navy operations, the best example being the "T" Attack Force, a joint navy-army air unit formed in 1944 that specialized in all weather and night attacks.

Besides these army systems, Central Bureau was responsible for breaking the Japanese naval land-based air-ground systems. This apparent anomaly resulted from the U.S. Navy's decision to concentrate its energies against Japanese carrier based air codes and major Japanese naval ciphers, such as JN-25B. For those reasons, it was content to have Central Bureau with its Australian and American army and air force personnel work the Japanese naval land-based air-ground communication system.[42]

The Australian navy detached its most experienced Japanese cryptologist, Commander Eric Nave, to Central Bureau in April 1942 to organize and supervise work against this system. Throughout the war in the Pacific, Australian army and air force field intercept sites had two components - an intercept section and an intelligence section. Together they shouldered much of the burden of intercepting,

---

[40] "Central Bureau Technical Records, Part B - Naval Air-Ground Communications," 37, Australian Archives (Victoria): Central Bureau, CRS B5436/1, Technical Records 1945-1946, Item No. IT B, 49. Hereafter cited as CBTR, B.

[41] CBTR, C, 5.

[42] CBTR, A, 2. I should observe that the Australian Navy's "Y" organization and the U.S. Navy Fleet Radio Unit, Melbourne (FRUMEL) operated independently of Central Bureau and analyzed a totally different set of naval cryptographic systems.

decoding, and disseminating intelligence derived from traffic analysis or decoded Japanese naval land-based tactical aviation messages. Japanese radio operators dispatched these coded messages in the complex Japanese version of Morse Code. The Japanese had, and still have, their own form of Morse Code, the so-called kana Morse based on the Japanese syllabary. That meant that an Allied intercept operator had to learn 73 kana Morse symbols, to ignore international Morse Code procedure, and cope with the great speed – 40 to 50 words per minute – of Japanese operators.[43]

The Japanese navy employed three different codebooks for its land-based air fleet. They were a transport code (three-kana symbol code), a general operations (a three-kana code), and a reconnaissance code (four-kana). Frequent triweekly changes were intended to preserve the integrity of these kana codes.[44] A weak point was the navy's use of Roman letter codes for destinations, probably the best known being "AF," meaning Midway Island. A typical message was encoded as follows. See Figure 5.[45]

An example of 3-kana operational code

Plaintext: " RR Hatsu PT Ni "
Literal translation: (RR [Rabaul] departed PT [Truk] for)
Correct translation: "Departed Rabaul for Truk."

PLAIN		CODE
R	=	TSU RO HI
R	=	TSU RO HI
Hatsu	=	A SA GO
P	=	KE KI N
T	=	NO KI MI
Ni	=	MU KA U

Encoded version: "TSU RO HI \ TSU RO HI \ A SA GO \ KE KI N \ NO KI MI\ MU KA U"

The earliest land-based naval air code system Central Bureau tackled was the Yo transposition system which appeared in June 1942 and ceased that October. Australian codebreakers at Central Bureau headed by Captain Nave did almost

[43] For a good first-hand description of Japanese manual Morse procedures see Jack Bleakley, *The Eavesdroppers* (Canberra, Australia: Australian Government Publishing Service, 1991), 8. Bleakley served as a radio intercept operator in Australian signals intelligence during World War II.

[44] Ibid., 74.

[45] Ibid.

all of the work against land-based naval air. They were so successful that when a codebook was recovered from a naval bomber downed near Dobodura, Papua New Guinea, in October 1943, Australian codebreakers had already recovered most of the values.[46]

By October 1944, two different four-kana books were in use, one for general use in sending naval operational traffic to and from air cover for convoys. Air cover over convoys to ward off Allied submarines unwittingly betrayed the convoys to Allied cryptanalysts by passing position reports.[47]

A Sample Solved Message

CODED MESSAGE	DECODED MESSAGE
SE NO SU	Sendan*
MU U TE	no
MU KU NO	ichi
TSU RO HI	R
TSU RO HI	R
YA YU TI	kichi
TO MO TI	32
TSU RI NE	6
MO SHI HE	50 (miles)
YA SU KE	shinro
MU KA NU	355 (degrees)
CHI HO SO	sokuryoku
YA HO NA	8 (knots)

*Sendan, the Japanese word for "convoy" always proceeded the message as the designation for convoy escort messages.

English translation: "Position of convoy: Bearing 326 degrees, 50 miles from Rabaul base - course: 355 degrees, speed 8 knots."

Reading such codes enabled 6 Wireless Unit at Tacloban, Leyte, to receive credit for 17 Japanese ships destroyed during the Japanese attempts to reinforce their

[46] "Allied Land Headquarters, SWPA to Advanced Headquarters," 17 October 1943, Papers of Field Marshall Sir Thomas Blamey World War, 1914-1918, 1939-1945, AWM File 419/10/2, Item 2/52.9.

[47] Geoffrey Ballard, *On ULTRA Active Service: The Story of Australia's Signals Intelligence Operations During World War II* (Richmond, Victoria, Australia: Spectrum Publications Pty Ltd, 1991), 166. Ballard served in Australian signals intelligence during World War II. Bleakley, *The Eavesdroppers*, 197; and CBTR, B, 25.

Leyte garrison through the port of Ormoc.[48] The other four-kana system was used only in the Philippines and Formosa. Japanese reconnaissance aircraft and strike aircraft trained to attack warships used this code.[49]

The Japanese navy also churned out encoded weather reports like those transmitted from its navigational aid stations to 11th Air Fleet Headquarters at Rabaul. Weather reports followed a set pattern which made solution a quick affair, despite frequent code changes. The weather reports informed Allied air forces of the weather over various Japanese targets and were helpful in deciding whether or not the meteorological conditions over a selected target were suitable for an attack.[50] For their part, Japanese special weather reconnaissance flights that reported conditions over Allied bases invariably occurred earlier in the day of a scheduled attack. A typical coded message might be transmitted as follows (see Figure 5):[51]

The best indicator of an imminent air raid in the Southwest Pacific Area, however, was the Japanese habit of having three major radio stations rebroadcast to operational commands the reports from the weather aircraft. Since this was the only occasion on which these stations passed weather reports in a three-kana code, it was self-evident that an enemy air raid was imminent.[52]

Naval outposts used a simple combination of plain text and abbreviations to issue warnings. These usually consisted of a combination of Japanese plain language and abbreviations transmitted in a set pattern. A sample message; [53]

HI HI HI /HA 24/6/HO 1/MU MU HO 5/0700/KE YO NI

Three kana group	HI HI HI	Enemy aircraft sighted
Type of aircraft	"HA" 24	"B" 24
Number of aircraft	6	6
Direction of sighting	HO 1	In the north
Course of a/c	MU MU HO 5	Heading south
Time of origin	0700	0700
Originator	KE YO NI	Sub-unit of Base Force 24 at Saumlakki, Tanimbar Island.

[48] CBTR, B, 25. Bleakley, 186-187. Ballard, 222.

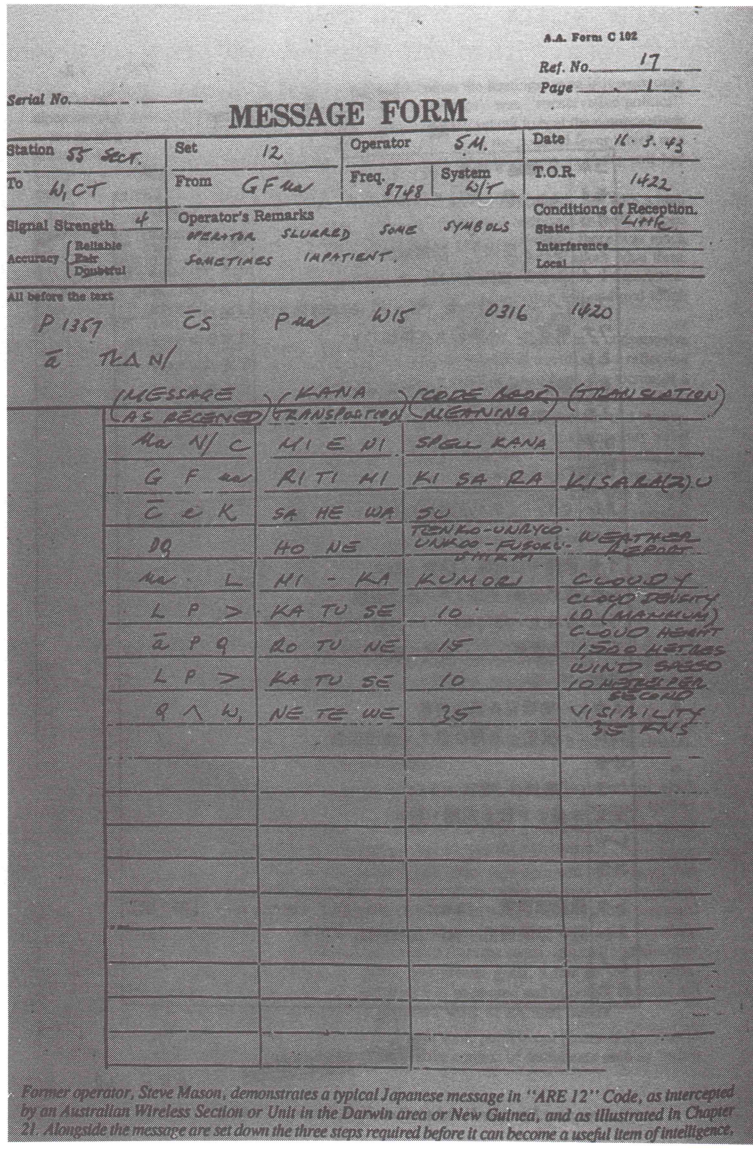
[49] CBTR, B, 10.

[50] CBTR, A, 6.

[51] Ballard, second illustration following page 186. I am grateful to Mr. Ballard for his kind permission to reproduce this illustration.

[52] "Central Bureau to CO 1 WU, Townsville, CO Fordet Port Moresby," 26 March 1943 cited in Bleakley, 82-83.

[53] CB, B, 32. The same source identifies KE YO NI at Saumlakki, Tanimbar Island, operating as a subsidiary outpost and radar site of Base Force 24 Detachment, Dobo, Aroe Island.



A.A. Form C 102
Ref. No. 17
Page 1
Serial No.

MESSAGE FORM

Station 55 Sect.	Set 12	Operator S.M.		Date 16.3.43	
To W.C.T.	From G.F.W.	Freq. 8748	System K/T	T.O.R. 1422	
Signal Strength 4	Operator's Remarks: OPERATOR SLURRED SOME SYMBOLS SOMETIMES IMPATIENT.			Conditions of Reception. Static Little	
Accuracy: Reliable / Fair / Doubtful				Interference	
				Local	

All before the text

P 1367 CS P.W. W15 0316 1420

ā TKA N/

(MESSAGE AS RECEIVED)	(KANA TRANSPOSITION)	(CODE BOOK MEANING)	(TRANSLATION)
Ma N/C	MI E NI	SAGU KANA	
G F W	RI TI MI	KI SA RA	KISARA(?)U
C E K	SA HE WA	SU	
DQ	HO NE	TENKO-UNAYCO-UNKOO-FUSOKU-UMARI	WEATHER REPORT
W L	MI - KA	KUMORI	CLOUDY
L P >	KA TU SE	10	CLOUD DENSITY 10 (MAXIMUM)
ā P Q	RO TU NE	15	CLOUD HEIGHT 1,500 METRES
L P >	KA TU SE	10	WIND SPEED 10 METRES PER SECOND
Q ∧ W	NE TE WE	35	VISIBILITY 35 KMS

Former operator, Steve Mason, demonstrates a typical Japanese message in "ARE 12" Code, as intercepted by an Australian Wireless Section or Unit in the Darwin area or New Guinea, and as illustrated in Chapter 21. Alongside the message are set down the three steps required before it can become a useful item of intelligence.

Figure 5. A typical Japanese naval weather message as intercepted by 55 Australian Wireless Section. Note the tranposition step required to reach the codebook meaning.

From On ULTRA Active Service by Geoffrey Ballard - with permission.

Given the numbers of codes, encipherment systems, conversion squares, and complicated communications' procedures, is it any wonder that Kamaga and the Japanese army believed that its codes were secure? Indeed some were, others were less so, and still others almost insecure. Still it is important to realize that the major four-digit systems were secure through April 1943, when 2468 fell victim to Allied cryptanalysis. The army's general-purpose code system kept its secrets effectively until the capture of the code library of the 20th Infantry Division. Recall also the Allies' inability to solve the Japanese army's main tactical cipher. Yet the Japanese army air force's 3366 code system was compromised, as were just about all lower grade systems employed by the Japanese navy's land-based air arm and the Japanese army air force as well as weather and outpost codes. Neither complexity nor code multiplicity ensured lasting communications invulnerability; the security of Japanese army codes fluctuated according to time, place, system, and circumstances. So the answer to the question of the title is, "It depended."

APPENDIX

A Partial List of Japanese Codes

Name /Edition	In Effect	Description
Rikugun angōsho 3	1 Jul 41	Army four-digit General Purpose Code
Rikugun angōsho 4	1 Jun 43	Army four-digit General Purpose Code
Rikugun angōsho 5	1 Jan 45	Army four-digit General Purpose Code
Kū-chi renraku kanjihyō 1	10 Jul 41	Army air force three-digit Air-Ground Code
Kū-chi renraku kanjihyō 2	1 Nov 42	Army air force three-digit Air-Ground Code
Kōkū angōsho 2	10 Jul 41	Army air force four-digit Ground Unit Code
Kōkū angōsho 2	1 Aug 44	Army air force four-digit Ground Unit Code
Kōkū hoan angōsho 1	Jul 41 ?	Army air force four-digit Garrison Code
Hikōbutai kanjihyō 1	Jul 41?	Army air force four-digit Antiaircraft Code
Hikōbutai kanjihyō 2	1 Aug 44	Army air force four-digit Antiaircraft Code
Hikōbutai kanjihyō 3	1 Jan 45	Army air force four-digit Antiaircraft Code
Geographic Place Name Code 1	1 Dec 42	Roman letter code
Geographic Place Name Code 2	1 Aug 45	Roman letter code
Butai angōsho	Dec 41	Unit Code Name and Number Code
Butai kanjihyō 2	Dec 41	Army three-digit Regimental code
Butai kanjihyō 3	1 Aug 45	Army three-digit Regimental code
Tsūshin angōsho 2	Dec 41	Army four-digit Communications Liaison Code
Atena angōsho 3	Dec 41	Army four-digit Ground/Air Address Code
Atena angōsho 4	?	Army four-digit Ground/Air Address Code
Atena angōsho 5	1 Aug 45	Army four-digit Ground/Air Address Code

Tsūshin butai angōsho	?	Army four-digit Communications and Commanders' Code
Kempei angōsho 2	Dec 41	Military Police four-digit Code
Kempei angōsho 3	1 Jul 43	Military Police four-digit Code
Senpaku angōsho 1	Dec 41	Army four-digit Water Transport Code
Senpaku angōsho 2	?	Army four-digit Water Transport Code
Senpaku angōsho 3	1 Jun 45	Army four-digit Water Transport Code
Kyōdō sakusen angōsho 3	Dec 41	Joint Operations four-digit Code
Kyōdō sakusen angōsho 4	?	Joint Operations four-digit Code
Kyōdō sakusen angōsho 3	1 Jun 45	Joint Operations four-digit Code
Kyōdō chimei jiten	1 Apr 45	Joint Place Name Code
Naval land-based, air-ground transport code		Three-kana Code
Naval land-based, air-ground operations code		Three-kana Code
Naval land-based, air-ground operations code	Oct 44	Four-kana Code (two books; one limited to Philippines/Formosa areas; one for air cover for convoys)
Naval land-based, air-ground reconnaissance code		Four-kana Code
Naval weather code		Three-kana Code with plain language
Naval observation posts reporting code		Three-kana Code with plain language

BIOGRAPHICAL SKETCH

Edward J. Drea is the Chief, Research and Analysis Division, U.S. Army Center of Military History, in Washington DC. After military service as an intelligence officer in Japan and Vietnam, he returned to graduate school and received his PhD in modern Japanese history from the University of Kansas. He is the author of *MacArthur's ULTRA: Codebreaking and the War Against Japan, 1942-1945*.

THE AUTOSCRITCHER

C. A. Deavours

ADDRESS: Mathematics Department, Kean College of New Jersey, Union NJ 07083 USA. Internet: deavours@luau.kean.edu

ABSTRACT: In the latter part of WWII, the Army Signal Security Agency built several machines known as Scritchers. These machines mechanized the solution of a variant of the German Enigma cipher machine having a rewirable reflecting rotor. This article discusses the probable method by which the machines worked.

KEYWORDS: Enigma, Scritcher, Autoscritcher, Bombe.

INTRODUCTION

In 1992, David Crawford and Philip Fox published an article, [1], in which they described two versions of a cryptanalytic device built by the Army Signal Security Agency. The first of these "scritchers" was a relay based device while the second machine was a faster electronic version of the first. However, both machines used copies of the five German Army Enigma rotors in their operation. The reader is referred to [1] for a detailed design description of both devices.

The scritchers were built and housed at Arlington Hall Station, as were other cryptanalytic machines built by the Army. The autoscritcher seems to have become operational in the 1944-45 period while the Superscritcher was in use from early 1946. Crawford, Fox, and others were a part of F Branch at Arlington Hall. This section was then under the command of Colonel Leo Rosen who had, as a young Signal Corps Lieutenant in the late '30s, suggested the use of stepping switches for mechanizing the solution of the Japanese Purple machine [2, p. 238]. The engineers working on the scritchers were never told exactly what cryptanalytic problem was being attacked by the system other than that the German Enigma cipher machine was the intended target of the analysis. The purpose of this article is to describe, in more detail, the method of cryptanalysis implemented by the scritchers as well as the primary problem that was attacked.

The cryptologic ingenuity of German designers is well known [2, Chapter III]. Among the "Enigma variations" produced was a version of the Enigma having a rewirable reflecting rotor [2, p. 138]. "Scritching" was a method of solving the

ciphers generated by this variant of the Enigma family of cryptographs. The bombe devices constructed by the British and Americans could not deal with the ciphers produced by the rewirable reflector since those machines relied on the wiring of all rotors, including the reflector, being known before a problem could be attacked. The fact that the first device built was known as the "auto"-scritcher indicates that scritching was not new but that the process was being automated for the first time.

The method of scritching uses a "meet-in-the-middle" type of cryptanalytic attack and can be conceived as having evolved from the earlier Method of Batons used to attack commercial versions of the Enigma. Like most machine analysis methods of that time, a break in the system was initiated using a plaintext crib. It seems at this point that the amount of matching plaintext and ciphertext required was large, perhaps in the range of 150-200 letters. This requirement in turn indicates that the rewirable Enigmas were probably used in communications circuits where the regular version of the machine was also employed. This fact would have resulted in lengthy plaintext cribs becoming available when a message was encrypted and transmitted using both versions of the machine and solved for the simpler system.

To understand how the scritching technique may have evolved, consider the following Enigma crib which might constitute the beginning of a cryptogram (German plaintext with "X" for word division).

CIPHER: Y Q P J Z N V K I R O W E W S Y X Y O Z C Y Y I Z X E
PLAIN: V O N A U F K L X A B T X D R E I A N D R E I X D I V

The equation governing the machine is

$$pPC^iRC^{-i}C^jSC^{-j}C^kT^{-k}UC^iTC^{-i}C^jS^{-1}C^{-j}C^kR^{-1}C^{-k}P^{-1} = c$$

where p denotes a plaintext letter, c, the corresponding cipher letter, R, S, T are the fast, medium, and slow rotors respectively, positioned at i, j, and k, U is the reflecting rotor and P is the plugboard permutation.

The operator C^i denotes, as usual, a circular shift of i letters forward in the A-Z alphabet.

This equation can be written as

$$pPC^iRC^{-i}C^jSC^{-j}V = cPC^iRC^{-i}C^jSC^{-j} \tag{1}$$

where $V = C^kTC^{-k}UC^kT^{-1}C^{-k}$ is the permutation induced by the slow and reflecting rotors in combination. We shall call V the "crossover permutation" or "crossover wiring". It should be observed that V is idempotent (self-reciprocal)

since $V * V = I$. In words, equation [1] asserts that if we encipher both p and c first using R and then S to obtain p' and c' respectively, then the results are related the equation

$$p'V = c'.$$

As long as the slow rotor, T, does not move, V remains constant.

PLUGBOARDLESS SCRITCHING

Suppose that, in the previous crib, we knew which rotors were the fast and medium rotors, and, in addition, the plugboard was left unplugged ($P = I$), then we could encipher both plain and ciphertext starting at the correct rotor positions and stepping the medium rotor at the appropriate point to obtain the p' and c' strings. In this particular case, we would have

```
CIPHER: Y Q P J Z N V K I R O W E W S Y X Y O Z C Y Y I Z X E
    c': D P A D U P Z K X J G U R A L V F B T H X E G G G Q U
    p': U R I U X R C E Q V S D P I W J M Y H T Q K S S S X D
 PLAIN: V O N A U F K L X A B T X D R E I A N D R E I X D I V
```

By reading the c' and p' lines we see parts of the (reciprocal) V permutation, e.g. DU, PR, AI, UX, etc. In fact, the repetition of some of the 13 pairs constituting the V mapping is evidence that the correct rotors and starting positions and turnover point have been chosen. If we had selected the wrong rotors and/or starting positions, we would have obtained something like the following sample.

```
CIPHER: Y Q P J Z N V K I R O W E W S Y X Y O Z C Y Y I Z X E
    c': A D N S T U B N P F Y L B R X Q I P K J E J R H H U E
    p': Q X O W H T V D O E G F K H J O N J P X W W Y U J G S
 PLAIN: V O N A U F K L X A B T X D R E I A N D R E I X D I V
```

In this second case, the p' and c' lines contain numerous contradictory pairings such as DX/XJ, YJ/YR, XS/XU, EE. This observation can be developed into a method of cryptanalysis.

To determine the identities of the fast and medium rotors and their starting positions, we could take our plaintext crib and encipher both strings using assumed identities for the fast and medium rotors as well as assumed starting positions for these rotors. The resultant enciphered strings constitute "deductions" about the crossover permutation, V. If we had an N letter crib, we would then have N enciphered pairs of letters. If any of the letter pairs contain contradictions, as was seen above, then, the rotors used or the starting positions must be invalid. When the true rotor order and starting positions are tested,

we would see no contradictions in the enciphered pairs and, moreover, we would probably see some of the deduced pairs repeated if the crib is long enough. This latter phenomenon of a repeated deduction is termed a "hit". Of course, we can also expect some number of false alarms, settings that satisfy all our selection criteria but are nevertheless incorrect, in this process. It is also necessary that the stepping position of the medium rotor be known - something which is not too difficult to determine in this case.

Using the principles discussed in reference [1], we can show how an ingenious machine using stepping switches, rotors, ' wiring, and associated control circuitry may be constructed to perform the above process. A simplified diagram of the device is shown in Figure 1. In the illustration, the stepping switches and rotors have only 4 positions instead of the 26 positions that would be necessary.

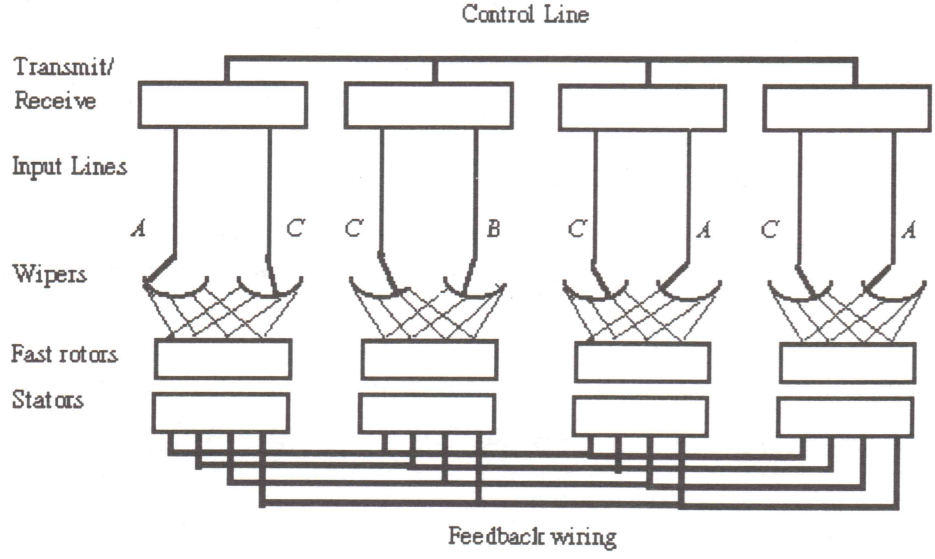


Figure 1. Hypothetical Scritcher with 4 Plain/Cipher pairs.

In general, we would have N two-rotor sets. Each rotor set contains the same two rotors in the same order but set to different positions. The input to each rotor set is via two input lines determined by the settings of the two stepping switches shown. The wiring from the 26 position stepping switches to the 26 rotor contacts is such that the "A" positions on both switches are wired to the "A" rotor entry position, the "B" positions are wired to the "B" entry points and so on. Electrical signals input along the two input lines selected by the stepping switches then pass through the two rotors representing the fast and

medium rotors in the Enigma machine. Upon exiting the second rotor, the two output signals are fed back into each of the other rotor sets and traverse these rotors in reverse order.

Thus, if we were to send pulses through the two input lines selected for the first set of rotors, then, the two signals exiting from that rotor set constitute a crossover wiring deduction. This deduction is tested for consistency by feeding it into every other rotor set. If there is another rotor set that would have "deduced" the same crossover wiring, then, this fact can be determined by the presence of current in both of input lines of that rotor set. In other words, we "pulse" each of the rotor sets one at a time and look for the presence of current in the two input lines of all of the other rotor sets. A hit is scored when we detect current simultaneously in both input lines of any other rotor set.

If none of the other rotor sets indicate the presence of current in either of their input lines, then, there is no contradiction in the deduced crossover wiring (but no confirmation either). In the case that current is sensed in only one of the two input lines of another rotor set, then, a contradiction has been deduced.

It should now be clear how to use this device to determine the correct rotor order and positioning. First, the two rotors to be tested are chosen and inserted into the machine. Next, the pairs of wipers for each of the N sets are set to correspond to the known plain/cipher pairs of the crib. The positions of the rotors must be set according to same arbitrary starting point taking into consideration the stepping position of the medium rotor (as shown below). Finally, we need to run the rotors through all possible positions and to test at each position for hits and/or contradictions.

FAST																													
	1	1	1	1	1	1	1	1	1	1	2	2	2	2	2	2													
POS:	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	0		
CIPHER:	Y	Q	P	J	Z	N	V	K	I	R	O	W	E	W	S	Y	X	Y	O	Z	C	Y	Y	I	Z	X	E		
PLAIN:	V	O	N	A	U	F	K	L	X	A	B	T	X	D	R	E	I	A	N	D	R	E	I	X	D	I	V		
MED:	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1		
POS											(Stepping position for medium rotor)→																		

Instead of rotating both rotors while keeping the stepping switches locked at their starting positions we may also keep the medium rotor fixed (stator) and rotate only the fast rotor. In this case, the stepping switches must be passed through all 26 possible positions with each pair of switch wipers maintaining the same distance apart as in their initial setting. This latter procedure was the stepping method used by the Autoscritcher and the Superscritcher.

When the second rotor is fixed in a static position, the solution is obtained is a relative one. For example, suppose the correct starting positions of the fast and medium rotor were "H" and "X" respectively. (This means that the fast rotor

is actually at position "Y" when the first letter is enciphered.) Further, assume that the first three matching plain/cipher pairs of the crib were VY, OQ, and NP. If we fix the medium rotor at position "A" then the solution will be found when the fast and medium rotors are at positions "R" and "A" respectively. This is because the distance from "Y" to "H" is 9 letters. Therefore, if the medium rotor is fixed at position "A" the relative displacement between the two rotors must be the same at the solution point. The distance between "R" and "A" is also seen to be 9 letters. This will also cause the stepping switch wiper positions at the solution point to be shifted 9 letters forward. The wiper positions at the solution will be EH, XZ, and WY. The reason for this phenomena can easily be seen mathematically.

If

$$pPC^iRC^{-i}C^jSC^{-j} = p' \tag{2}$$

then,

$$pPC^iRC^{-i}C^jS = p'C^j,$$

which can be written,

$$pC^jC^{-j}C^iRC^{-i}C^jS = p'C^j$$

or,

$$pC^jC^{(i-j)}RC^{-(i-j)}S = p'C^j. \tag{3}$$

In Equation 2, rotors R and S are at positions i and j respectively. In the equivalent Equation 3 S is at rotor position 0, i.e. "A", while rotor R has been shifted backwards j positions. Note that p and p' are both shifted forward by j positions. These two equations also show that hits remain hits and contradictions remain contradictions when the medium rotor is fixed during the search process although the deduced crossover wiring pairs are all shifted forward as are the original plain/cipher pairs as represented by the setting of the stepping switch wipers.

THE AUTOSCRITCHER

When the principles of the forgoing hypothetical machine are understood, the operation of the Autoscritcher and its more electronic counterpart, the Superscritcher, can be understood easily.

Extending the previous crib into a full text and enciphering it with the same settings but now using plugboard connections as well, we have

```
                                1 1 1 1 1 1 1 1 1 2 2 2 2 2 2
  0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5
0 R Q Z J I N D U I Y I C E C W R X R O P F R R I P X
  V O N A U F K L X A B T X D R E I A N D R E I X D I

1 E H F Y G Q H H U Z T E A C X L A M R G W M D D L O
  V X S C H W A C H E X F E I N D L X X K R A F T E X

2 W G M R H P U R Y T N U R S T L Y Y A D K N M Q H A
  S U D L X H O H E X Z W O X V I E R X A C H T X A N

3 F P F T P J G W L L B P E N N T X X V Y P V G V R X
  Z W O X V I E R X A C H T X F E S T G E S T E L L T

4 U P Y D R M Y O V S U T Y M T L S F R W V B Q F L U
  X X M I N E N S P E R R E X N O R D A U S G A N G X

5 J M E N H R S C H P W
  E I C H W A L D E X X.
```

The fast and medium rotor positions have been numbered relative to the arbitrary points 00 (i.e., "AA"). The assumed stepping position of the medium rotor is also indicated.

We cannot proceed as previously in this case because the unknown plugboard mapping prevents us from enciphering our crib correctly. The crib contains a number of plain/cipher pairs in which the same two letters are paired. Some of these are shown in boldface. Extracting four of the most frequent such pairs and noting the positions of their occurrences we have

XT	EY	AR	NF
10-1	8-2	17-0	5-0
9-2	16-2	18-4	14-3
3-3	19-3	5-5	23-4
17-3	12-4		
25-4			

These four sets of data are now treated as four "groups" by the Autoscritcher. In each of the four cases we have a letter pair such as XT which has been enciphered by the plugboard. The Autoscritcher attempts to find the plugboard connections for each pair of letters in a given group using much the same techniques as before to check for hits and consistency between the groups. To begin, the rotors are all set up according to the relative positions shown above. The modifications from our previous method are easy to see. For each group we try all possible combinations of plugboard combinations. This means that the wipers must try all 26×26 possible positions for each pair of letters. In contrast to our

previous attack, all wiper positions are the same at all times for the rotors in a given group since the same plugboard mapping must work simultaneously for all rotor pairs in the group. When a hit is attained for a rotor position and wiper positions in group 1, then, we attack group 2 the same way by trying all possible plug connections. If we fail to find any usable wiper positions at some group i, then, we go back to group $i-1$ and continue from where we left off searching. If no viable solutions are found after all 26 settings of the fast rotor are tried, then, the rotor set is changed and the search continues.

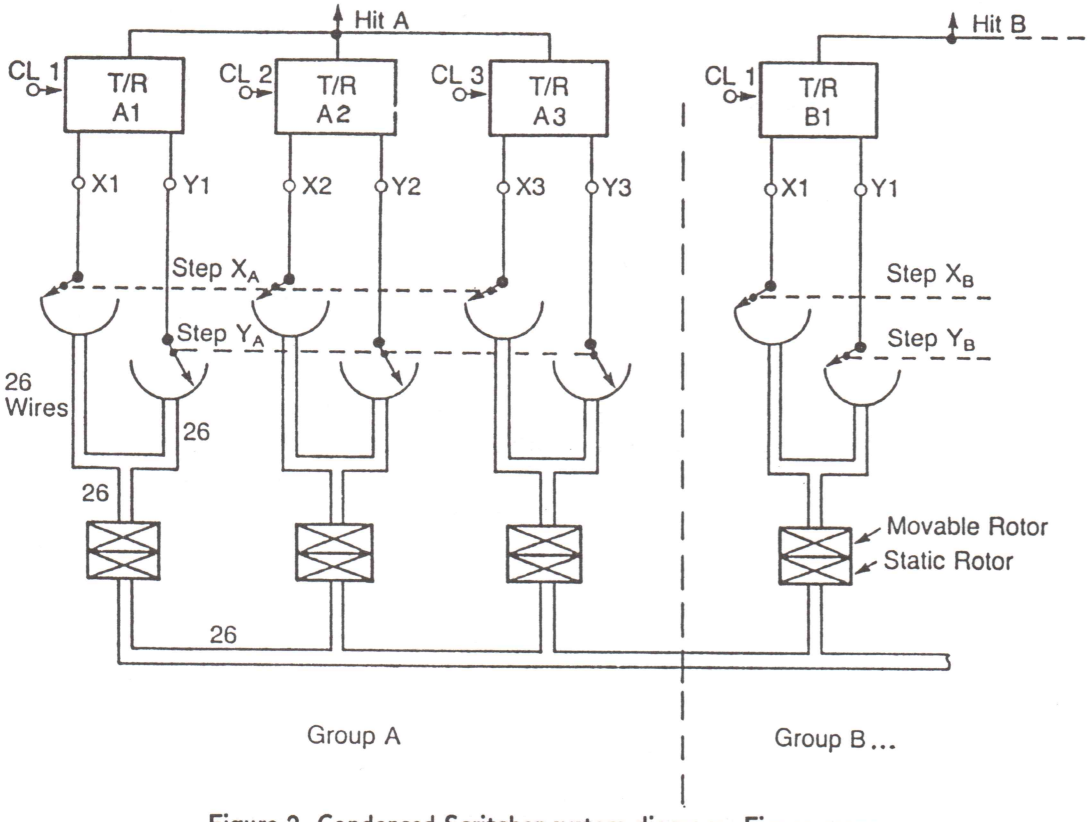


Figure 2. Condensed Scritcher system diagram. Figure reproduced with permission from [1], Copyright 1992 IEEE.

SEARCH LOGIC

The description given here of the search logic used in the Autoscritcher differs in important ways from that described in reference [1] which was, admittedly, based on memories recalled from decades before. As described in the referenced paper, the machine seeks a hit in the first group. When a hit is found, the first group

search halts at its current positions and the search continues with the second group with the search surging back and forward between groups until a hit is recorded in all groups. The scritcher diagram accompanying the article is shown in Figure 2. There is no interplay between the groups and the 26 wires that connect all of the rotor sets in Figure 2 are for "convenience only". A typical set up involved 5 rotor sets with the number of rotors in each set going from about 7 down to 3. Thus, five groups with 7, 6, 5, 4, and 3 rotors might be considered normal.

With no interconnection between the groups, the Autoscritcher could never have delivered a solution. Not only is there a serious problem with false alarms, but, the true solution would never emerge. To see why this is so, consider the fact that when we have a group of N rotors at the correct settings, the probability that two randomly selected crossover deductions will coincide is about 1 in 13. Since there are $N(N-1)/2$ such comparisons, the expected number of hits is given by $N(N-1)/26$. So, the expected number of hits in the above situation is given by the following.

N	Expected Hits
7	1.6
6	1.2
5	.8
4	.5
3	.2

Clearly, it is only remotely possible for all 5 groups to score hits simultaneously. For proper functioning of the scritcher, it would seem necessary that hits are based on comparisons with all previous groups and not just within a single group. But, even this modification, while it would assure the correct solution would be found with high probability in the above case, would leave too many false alarms with which to deal. The logic used in the machine must also have rejected cases where only one input line of a previous or current rotor set sensed current. Without this additional proviso, the correct solution is literally buried among hundreds of false alarms.

There are other types of restrictions that could have further reduced the probability of false alarms. For example, if all the plain/cipher pairs used are chosen so that no letter occurs more than once in the complete set of pairs, then we can assert that the plugboard deductions must all contain distinct letters. In reality, I doubt that this condition, which would check to see that no two wipers between the groups were ever positioned at the same setting, was implemented.

The article further notes that all possible 26×26 wiper settings for a group were explored in seeking a solution. This exhaustive attack would be unnecessary

since, if a wiper setting, say X/Y is valid, then so is Y/X. For each setting of one of the two stepping switches, the other switch only has to try the next setting up to the last setting. This means that, for one switch at setting A, the second switch must try settings B-Z. When the first switch is at setting B, the second switch must try C-Z, etc. The number of combinations that need to be tried in this case is $25 + 24 + 23 + ... + 1 = 325$ instead of $26 \times 26 = 676$.

SAMPLE SOLUTION

In order to study the scritching process more thoroughly, a simulation of the machine was written in BASIC. (This program is offered as freeware to readers.) When the four sets of group data for the above cryptogram were entered and the program was run, a solution was obtained with the fast rotor being Enigma rotor III and the medium rotor being Enigma rotor II. The solution was attained at a fast rotor setting of "R" and the (fixed) setting of "A" for the medium rotor. The wiper positions at the solution were EA, LY, HF, and UM. The deduced crossover wiring connections were as follows:

GROUP	CROSSOVER DEDUCTIONS:				
XT	JG	IF	KB	TM	BK
EY	YW	HP	FI	AO	
AR	IF	JG	RL		
NF	YW	MT	CQ		

We can see that 8 of the 13 distinct mapping pairs of the crossover permutation, V, have been deduced in the solution process. By examining the above list, it can be seen just how the solution was attained. A hit, "KB" was scored in the XT group. A hit in Group 1 is necessary to get the solution process started. The EY group had no hit within itself, but, it did have one in comparison with the previous XT group deductions, namely, "IF". The solution process then continued with two hits in the AR group ("IF" and "JG" from the XT group. Finally, the hit "MT" was scored between the NF group and the XT group. Since there were no contradictions encountered, the program stopped at these settings. A number of false alarms were also encountered due to the paucity of the data used.

The reader may wonder if the "relative" solution achieved about can be translated into "absolute" form. In this case, the answer is affirmative. If the four solution wiper settings are backed up, the correct value is easily seen because only 6 plugs were used in this cryptogram leaving 14 letters unchanged by the plugboard.

SOLUTION	EA	LY	HF	UM
-1	DZ	KX	GE	TL
-2	CY	JW	FD	SK
-3	BX	IV	EC	RJ
-4	AW	HU	DB	QI
-5	ZV	GT	CA	PH
-6	YU	FS	BZ	OG
-7	XT	ER	AY	NF

At the last position the correspondence between these values and the starting plain/cipher pairs of the crib is apparent. We have

P/C Pairs	Soln - 7
XT	XT
EY	ER
AR	AY
NF	NF.

This last comparison shows that the letters X, T, E, A, N, and F are probably unchanged by the plugboard while another of the plugboard mappings is (Y, R). Since the original plain/cipher pairs have been shifted 7 letters forward after plugboard encipherment, the starting positions of the fast and medium rotors must be shifted forward 7 positions from RA to YH indicating that the fast rotor started at position X and the medium rotor at position H. The author does not wish to leave the impression that determining the absolute setting from a relative one is always so easy.

We see that the scritching solution process provides the identities of the fast and slow rotors along with the their relative displacements from one another as well as a set of plugboard and crossover wiring values. Generally, more than enough data is obtained in order to deduce the remaining values through trial and error.

CIPHERTEXT ONLY

A remaining question of interest is whether or not the ideas involved in scritching can be extended to provide a solution when no cribs are available. The logic involved in picking out a correct solution and rejecting incorrect solutions is considerably more complex (and thereby all the more interesting) than in the probable plaintext case. In view of this observation, it would probably be necessary to use a general purpose digital computer instead of a special purpose machine for the analysis.

If we know only ciphertext, then, we could extract the settings of identical letters and these would form our groups. When a correct rotor setting and the correct wiper position for a letter is attained the situation differs from our known crib case because a single wiper position in the second stepping switch will not correspond to all of the unknown plaintext letters. Analysis becomes more complicated, particularly the problem of rejecting false alarms.

FREEWARE

The Autoscritcher simulation, sample problems, and other related material is available from the author. Send a formatted DOS disk along with a self addressed return mailer to the author by the address given in the title to this article. (US residents only, please)

REFERENCES

1. Crawford, David and Philip Fox. 1992. The Autoscritcher and the Superscritcher: Aids to Cryptanalysis of the German Enigma Cipher Machine, 1944-1946. *IEEE Annals of the History of Computing*. 14(3): 9-22.

2. Deavours, Cipher and Louis Kruh. 1985. *Machine Cryptography and Modern Cryptanalysis*. Norwood MA: Artech House.

BIOGRAPHICAL SKETCH

C. A. Deavours is a Professor of Mathematics and Computer Science at Kean College of New Jersey. Aside from teaching and consulting, most of his time is spent directing the Mathematics Department computer network facilities.

IN MEMORIAM

SOLOMON KULLBACK

April 3, 1907 - August 5, 1994*

Solomon Kullback was the third cryptanalyst hired by William Friedman in 1930. Friedman was putting together a new cryptologic team made necessary by the collapse of Yardley's Black Chamber in 1929.

Kullback was born in Brooklyn on April 3, 1907. He went to school with Abe Sinkov, the second Friedman hiree, at Boy's High School in Brooklyn. Both were interested in mathematics, and both graduated in 1927 from CCNY with BS degrees in math. Both then obtained MA's in math from Columbia in 1929, and began teaching school. One day Sinkov came to Kullback with a civil service announcement of positions in mathematics in the Federal Government. Kullback was none too entranced with teaching, and neither was Sinkov, so they both applied.

Friedman initially rejected both for employment because, although they appeared to be brilliant math and science students, they were not that strong in foreign languages, the second requirement for the job. Eventually, however, Friedman buried his doubts about their language ability and hired them. He had already hired Frank Rowlett, so Sinkov and Kullback became the second and third "junior cryptanalysts" to join Friedman's team, at $2,000 per year (each).

For the next ten years the team of four (Friedman, Rowlett, Sinkov and Kullback) were the heart and soul of the Army's rudimentary cryptologic organization. Their highest priority target became Japanese diplomatic systems, and in 1935 they succeeded in reading traffic from Japan's first machine diplomatic system, which they called Red. This accomplishment was considered all the more

*Thanks to Jack E. Ingram, Curator and Historian, National Cryptologic Museum, for permission to publish this tribute to Kullback, which appears in the Museum.

difficult because they never actually saw a Red machine, and reconstructed it using mathematical cryptanalysis.

In 1938, the Japanese introduced a new machine system, more advanced than Red. They called it Purple. By this time, Sinkov was in Panama and Kullback was in Hawaii, to set up the Army's intercept capability. They were called back, however, and in 1940 the Army, with a team of cryptanalysts which included additional cryptanalysts, succeeded in reading Purple. Once again, they accomplished this without seeing a Purple device.

Through the war Friedman kept his team of civilians together to work on the high-priority Japanese and German systems, By this time Kullback, brought into the Army as a major, was one of the senior officials in the Signal Intelligence Service, a branch of the Signal Corps. He did most of his work on German systems, and was one of the first Army officers to make the trip to Bletchley Park to begin the liaison with the British, in 1942. At the end of the war he was a colonel and chief of the Military Cryptanalysis Branch in SIS.

After the war Kullback stayed on, first with ASA as the Chief of Research Laboratories. In 1949, when AFSA was created, he became the first Technical Director of Research and Development. Kullback retained that position in 1952, when he joined AFSA's successor NSA. Then in 1957 he became Assistant Director for Research and Development, and stayed in that position until his retirement in 1962.

Kullback was one of the most distinguished scientists ever to work in American cryptology. He obtained a PhD in statistics from George Washington University in 1934. He began teaching in GWU in 1938, on his return from Hawaii. Through the years he published three books and numerous articles on statistics and mathematics. When he left government, he joined the GWU faculty full-time, and from 1964 to 1972 was chairman of the department of statistics. He received the Legion of Merit from the Army, and when he retired from NSA, the Exceptional Service Award. When he retired again (this time from GWU) he became professor emeritus.

THE CRYPTOLOGIC ORIGIN OF BRAILLE*

David Kahn

ADDRESS: 120 Wooleys Lane, Great Neck NY 11023 USA.

ABSTRACT: Louis Braille's concept of raised writing for the blind stemmed from an army officer's system of writing in the dark (as of a dugout) and secretly.

KEYWORDS: Braille, Barbier

Louis Braille, inventor of raised-dot writing for the blind, got his idea from a secret communications system devised for military purposes by a French army officer, Nicholas-Marie-Charles Barbier de La Serre.

Barbier was born 18 May 1767 at Valenciennes, in the north of France. At 15, he was admitted to a military school under a provision allowing impoverished young noblemen to attend. The school was perhaps that at Brienne, where he would have been for a year a fellow student of Napoleon Bonaparte. He graduated as an artillery officer (as did Napoleon). When the French Revolution broke out, he emigrated to the United States, working as a surveyor and living with Indians until his return to France under Napoleon's empire.

He became interested in fast, secret writing and, in 1808, published a brochure entitled *Tableau d'expédiographie* ("Table of speedwriting") and, in 1809, his *Principes d'expéditive française pour écrire aussi vite que la parole* ("Principles of French Speediness for Writing as Fast as Speech"). The latter described a process that he called "impressed writing to replace the pen or pencil and to execute several copies at a time without tracing characters." Barbier was describing a writing that could be felt, perhaps recalling times when such a capability would have been useful for officers in the field to draft outgoing messages in the dark and perhaps to "read" incoming ones with their fingers.

Barbier refined his idea when he proposed setting out the 25 letters of the French alphabet in a 5×5 Polybius square and later what he considered as the 36 sounds of French (e.g., a, i, ch, e, ieu) in a 6×6 square. Each letter or sound could thus be replaced by a pair of numbers. He recognized that by changing

*This material is adopted from Pierre Henri, *La Vie et l'Oeuvre de Louis Braille, Inventeur de l'Alphabet des Aveugles (1809-1852)* (Paris: Presses Universitaires de France, 1952), Chapter III, "La Genèse du système Braille."

the pattern of letters or sounds in the square, he would have a system of secret writing useful for soldiers or diplomats. As a mere monoalphabetic substitution, it was not very secure; perhaps he recognized this, for he did not insist on it further. Instead, he combined his ideas of cryptography and impressed writing in a machine that indented the numbers onto paper.

In 1819, he displayed this device at an exposition in a Museum of Products of Industry temporarily installed in the court of the Louvre. A report by three scientists to the Academy of Sciences the following year discussed two systems used apparently by two models of the machine to die-stamp the numbers representing the lines and columns of the square. In one of them, three raised dots formed right or obtuse angles. In the other, raised dots were ranged on an axis to facilitate determining them. All of this was for the military; none was for the blind. But, at the same exhibition, students of the Royal Institution for Blind Children showed how they could read from books – huge bound volumes – printed with ordinary letters in high relief by running their fingers over the words. Barbier perhaps witnessed the difficulty they had in figuring out the letters. By 1821, an article in the *Mercure technologique* that discussed the military and diplomatic advantages of Barbier's system also mentioned that the Royal Institution for Blind Children had adopted it for instruction, and in 1822 an entire article dealt with the use of the system for the blind.

This system utilized two parallel columns of six raised points each. The number of points in the left-hand column indicated the line of the square table of sounds, the number in the right-hand column the position within that line of the designated sound. Methods were given to punch the points into the paper.

Braille, a compatriot of Barbier's but 42 years younger, modified this sytem into an alphabet utilizing an array of 2×3 locations, in one or more of which dots are raised to indicate letters. Thus to represent a, the dot in the left column at the top is punched out, the other seven positions being left unpunched, or level; for o, the first and third dots in the left column and the second dot in the right column are raised. The 26 letters are supplemented by a sign for capital letters and a sign for numerals, which are then represented by the letters from a to j.

Braille, himself blind, was thus both honest and generous when he said of Barbier in 1829 that "it is to his method that we owe the first idea of our own."

BIOGRAPHICAL SKETCH

David Kahn, a co-editor of *Cryptologia*, is the author of *The Codebreakers*.

A TURNING GRILLE FROM THE ANCESTRAL CASTLE OF THE DUTCH STADTHOLDERS*

Karl de Leeuw and Hans van der Meer

ADDRESS: Faculteit Wiskunde en Informatica UVA, Plantage Muidergracht 24, 1018 TV Amsterdam, THE NETHERLANDS.

ABSTRACT: In the archive of the Dutch Stadtholder William V an undated, unsolved message of unknown origin was found. This message is solved and placed in its historical context by correlating the contents of the message with known historical facts. It turns out to be an early example of a turning grille belonging to the correspondence of Stadtholder William IV.

KEYWORDS: Cryptanalysis, eighteenth century, Dutch history, Stadtholder William IV, transposition cipher, turning grille.

INTRODUCTION

The early history of cryptography cannot be based solely on an analysis of *printed* sources. Tempting though it may be to draw conclusions regarding the development of this field from classical masterpieces like those from Vigenère, Porta or others; they still have to be collated by an investigation into the actual use or application of the methods as described. This may lead to the conclusion, as Kahn has pointed out, that a complicated system like the Vigenère, while getting considerable attention in literature, was hardly ever used during the seventeenth and eighteenth centuries [13, p. 147]. It may equally show that some methods were applied only after considerable modification or even, that methods were applied long before its widely known description. This of course raises the problem of the interplay between theory and practice, or rather the question of whether these books played an innovative role in the development of cryptography or just a secondary one. There seems to be reason to assume the latter because the cryptographer of the early modern period was usually working on his own or within a small circle of colleagues and not allowed, or even inclined, to

*We are indebted to H. M. the Queen of the Netherlands for granting permission to do research in the Royal Archive.

communicate his insights to others than to those directly involved. This question can only be solved by an exploration of coded or enciphered documents still to be found in many archives. They can give us a picture of the role cryptography actually played and will enable us to put ideas derived from printed sources to the test.

Dutch records cannot be excluded from such a survey. During the seventeenth and eighteenth centuries Holland played an important role in the development of merchant capitalism. It was involved in almost every major European conflict, but it had no appetite for territorial expansion and did not even want to play an independent role in the balance-of-power-politics so typical of this period.[1] The Dutch Republic, as the country was known at the time, could not do without ambassadors in all major capitals but it lacked the political ambition to spend more money on them than strictly needed. The operating of the diplomatic service could be cheaply run by sending diplomatic dispatches using the ordinary mail and using couriers only exceptionally, very much unlike the ambassadors of the great powers [1, p. 136–137].[2] This required a rather intensive use of secret writing that became more or less customary during the last decades of the seventeenth century and that was greatly improved during the second half of the eighteenth century. The role of ciphers and codes in Dutch foreign policy can to a large extent be recovered from the archives of the so called "States-General," the principal government body and from those of the embassies.[3]

This survey should be supplemented by an investigation of the relevant material in the archives of the Dutch "Stadtholders": semi-heriditary commanders of the army and the fleet who also had an important say in foreign policy. The examination of these records is, for the historian of cryptography, the most rewarding of all because of its great diversity. It can tell us not only something about the workings of the Dutch Black Chamber, but it also can give a picture of the role cryptography played in wartime. Moreover it furnishes examples of coded or enciphered documents that played a role in the safeguarding of the

[1] With the exception of the last quarter of the seventeenth century when the country was governed by stadtholder William III of Orange who was to succeed to the British throne in 1688.

[2] This lack of willingness to spend money on courier services was not exclusively determined by the proverbial Dutch sense of economy. According to baron Fain [6] who acted from 1806 onwards as Napoleon's personal secretary, ambassadors of small nations hardly ever used couriers of their own. Their letters were systematically intercepted at the Paris central post office and constituted, once decoded, the most valuable source of information on foreign diplomacy for the French government.

[3] A separate article on the codes used by the States-General is in preparation. Interestingly enough, Dutch nomenclatures do not conform entirely to the general pattern. The principle of the two-part code, developed by Rossignol, seems not to have been known or appreciated until the second half of the 18th century. At an earlier stage secrecy was thought to be served best by the use of very large, one-part codes with many synonyms. Sometimes these could comprise of about ten thousand codegroups. For examples see: Algemeen Rijksarchief, eerste afdeling, familiearchief Fagel, inv. nrs. 1257–1266.

private interests of the Stadtholder and his family, in the Republic and abroad.[4]

In the archive of the last Stadtholder, William V, we found an unsolved message. It was stored with other ciphers and codebooks and had no reference either to sender or to adressee.[5] A reproduction of the document on which it was found is presented in Figure 1. From its appearance we concluded that it was enciphered with a turning grille.

Figure 1. Reproduction of document. (size reduction to 80%)

[4] For information concerning the Dutch Black Chamber see [21, p. 17–26; 2, p. 238–260; 5].

[5] Koninklijk Huisarchief, stadhouder Willem V, inv.nr. 339(7).

SOLUTION OF THE CRYPTOGRAM

The decipherment of the cryptogram did not present many difficulties. A glance at the letter distribution reveals a lot of ch's, k's and even an ck. It appears to be German and indeed, a closer look brings a few ü's (see end of third and seventh row). We also note some capital letters in the upper left hand corner. They look like 'CAVE' and for the moment mean nothing to us. As it turns out we will be able to interpret them after the solution of the message is completed.

When we scrutinized the cryptogram for a point of entry, we recalled the warning already given by Cardano to users of transposition ciphers. One should rewrite the message in such a way that the subsequent steps are indistinguishable [13, p. 144]. In the case of a turning grille, it is the turning operation that easily leaves traces in the form of different lines of writing. And indeed, this phenomenon is visible in this document. Looking at the first line we can see that [d, i, e] (1st, 5th and 11th position) are clearly at a lower level than the rest of the line.

On line six and following we find the most clear examples of a line of writing and we decide to start the analysis here. Denoting with (x.y) the y'th character on the x'th line (numbering from left to write and top to bottom), we collect e (6.8), i (6.10) and n (6.16). On the next line we easily continue with g (7.1), e (7.5), g (7.9) and a (7.13). On the eighth line the pattern is less clear, but we feel safe in taking g (8.8), e (8.12) and n (8.14) also. Together this results in the fragment "eingegagen". We suspect here the word "eingegangen", for which the missing n is supplied by either (8.1) or (8.4).

So the first entry yields a genuine German word. It is time for the litmus test, in the case of a turning grille this is the examination of the sequence of letters formed by the inverted positions. In the following table these are shown.

We get the text "bierwelchesi" which could tentatively be split up in "bier welches i". It sounds like good German but we are not sure how to place this 'beer' in a secret message to a royal person.

I	6.8	6.10	6.16	7.1	7.5	7.9	7.13	8.1/4	8.8	8.12	8.14
	e	i	n	g	e	g	a	n	g	e	n
II	9.3	9.5	9.9	9.13/16	10.4	10.8	10.12	10.16	11.1	11.7	11.9
	b	ie	r	w/a	e	l	c	h	e	s	i

First step in solution guessing 'eingegangen', I↔II = *inversion.*

Continuing the analysis we expand the fragment that begins on the sixth line with er (9.1), e (9.7), r (9.11), k (9.15), u (10.2), n (10.6), d (10.10) and i (10.14). This leads to "eingegangen ererkundi", which sounds a lot like "eingegangener

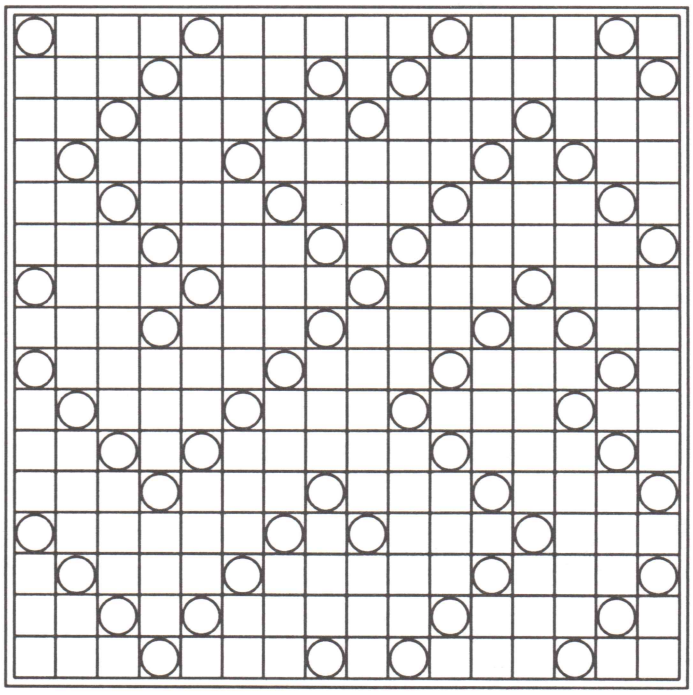


Figure 2. Key to the transposition.

erkundigung". This conclusion is reinforced by the position of the letters [g, u, n, g] on the next line. Again we seek the corresponding inverted positions, shown hereafter.

I	9.1	9.7	9.11	9.15	10.2	10.6	10.10	10.14	11.3	11.5	11.11	11.15
	er	e	r	k	u	n	d	i	g	u	n	g
II	6.2	6.6	6.12	6.14	7.3	7.7	7.11	7.15	8.2	8.6	8.10	8.16
	d	a	s	e	n	g	e	li	s	c	h	e

Second step in solution, I↔II = *inversion*.

The message is becoming more and more fascinating. We can now read the words "das engelische bier welches". There can be no doubt that we are solving the cryptogram but the contents become more and more intrigueing. We plod on in order to find out what all this about English beer is. After a while we arrive at the two fragments

> die franszosen sind laut eingegangener erkundigung und nachricht
> vielleicht fürchten sie das engelische bier welches ihnen wohl übel

and then the solution is quickly completed, the two other rotational positions of the turning grille supplying the rest of the information. The key to the transposition is shown in Figure 2. The solved message is as follows:

> die franszosen sind laut eingegangener erkundigung und nachricht von camberg abmarchiret es sollen aber dem verlaut nach andere an deren stelle einrucken vielleicht fürchten sie das engelische bier welches ihnen wohl übel bekommen durffte wan es recht getruncken wird ich wünschet dass sie die rechte maass bekommen mögten ⊖ koenig

DATING OF THE MESSAGE

The use of a turning grille would point to the end of the 18th century because of the known popularity of this device at that time. Most notable in this respect is the contribution in 1796 of C.F. Hindenburg [11], titled *Fragen eines Ungenannten über die Art durch Gitter geheim zu schreiben*, the oldest complete description of the turning grille and written nearly a century before the well-known description by Fleissner von Wostrowitz [7]. Moreover most ciphers and codebooks found in the archive of William V originate from that period.

Therefore it seemed very likely to us that the enciphered message had something to do with one of the wars caused by the French Revolution. The Dutch Stadtholder and his family were severely threatened by the new democratic tide that was flooding Europe. William V was nearly exiled by a Dutch democratic movement in 1787, but was at the last moment restored to power by the force of the Prussian army [14]. The Restoration Regime lasted only until 1795, when it was brought down by a French Revolutionary army. The Stadtholder was exiled to London and tried to protect his interests on the continent mobilizing an army of Dutch émigré's to reconquer the Republic.[6] The mention of French troops seemed to point in this direction too. Of course, the other data in the letter still had to confirm this interpretation.

Subsequently we looked at the word 'Camberg', apparently the name of a village or town but not a very well known one and probably not in the Netherlands either. It turned out to be a village in the west of Germany not far from the river Lahn and cities like Koblenz and Limburg.[7] In the 18th century it was part of the German possessions of the Dutch Stadtholders being from the line of

[6] A survey of this period in Dutch history is given by Schama [19].

[7] See the map. In this map Camberg is spelled Kamberg. It is located to the right and downwards from Nassau, at the point where the lines on the map cross.

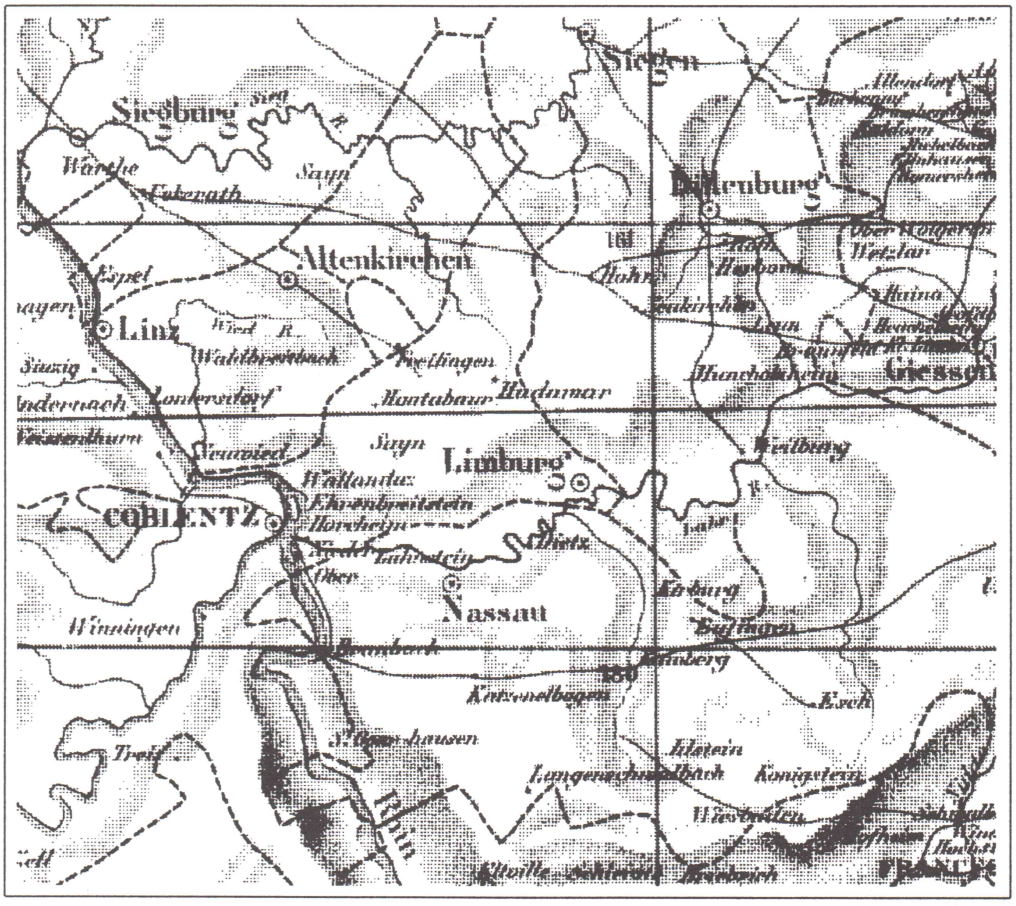


Figure 3. Area around Limburg a/d Lahn (Source: Royal Library, The Hague).

'Nassau-Dillenburg,' and their ancestral homeland. It provided them with the dignity of old nobility and with that of an independent ruler in the 'Holy Roman Empire of German Nations,' a loose confederation of states with an elected emperor at its head [12, p. 98–100; 17, p. 75-77]. This would account for the fact that the letter was found in the archive of William V in the first place, and gives a hint of where to look for the writer, probably to be found among the officials of this German principality.

To be more precise we had to check whether there were any French troops in or near Camberg at all and, if so, when exactly. This last question could be solved relatively easily. From a local chronicle we learned that there were actually French troops at Camberg in the period that we had expected them to be there: during the revolutionary era from 1797 until 1799. The French

had their commanding officers at nearby 'Oranienstein,' a beautiful barocque palace that was used as a residence by the Dutch Stadtholders when visiting their ancestral homeland [10, p. 18–40; 22, p. 33].

The next step was to find Mr. König. A list of civil servants of Nassau-Dillenburg showed that there was not one, but two officers called König strangely enough with the same initials. One was called Christian Andreas and the other Carl Anton. Suddenly the letters in the top left hand corner make sense. We should read them not as CAVE, but as CAK, the initials of both Carl Anton and Christian Andreas König. They both served as 'registrators' at the administration of the principality at Dillenburg, but not at the same time. Carl Anton was mentioned from 1751 until 1781 and Christian Andreas from 1780 until 1789. They were not mentioned later, that is to say in 1797 or 1798, but this need not necessarily mean that one of them could not have written the letter because these lists were not entirely reliable.[8]

Information from the 'Hessian State Archive' at Wiesbaden filled in the gaps. Carl Anton had already served the administration of Nassau-Dillenburg from 1744 onwards. He died suddenly in 1781 at the age of 71, his death being caused by a stroke.[9] His son, Christian Andreas, was born on the 30th November 1749. He was serving the administration from 1772 onwards, at first as a lawyer and proctor. In 1780 he became a registrator, like his father, and in 1782 he became his successor. In August 1789 he left the service of Nassau-Dillenburg to become a secretary at the Chancellary of Coppenbrügge, a town in northern Germany not far from Hannover.[10]

These results made the dating of the letter somewhere between 1797 and 1799 rather questionable. Of course Carl Anton could not possibly have written the letter during these years because he was no longer alive. But his son Christian was not likely to have written the letter either at that period because he no longer dwelled in the region.

A re-examination of the letter convinced us that we had been wrong. We had overlooked the importance of the part where the 'engelisches bier' was mentioned, apparently not liked by the French who were used to drinking wine. This statement could only have referred to stocks captured from British or at least Hannoverian troops, or perhaps to beer to be delivered to them by local breweries but confiscated by the French before it could reach its destination. This meant that the letter could not possibly have been written during the closing years

[8] Koninklijk Huisarchief, stadhouder Willem V, inv.nr. 339(31).

[9] Hessisches Hauptstaatsarchiv, Abt. 172, nr. 1902; Abt. 1001, nr. 61.

[10] Hessisches Hauptstaatsarchiv, Abt. 172, nr. 1905. We are indebted for this information to Mr. Eiler of the Hessisches Staatsarchiv.

of the 18th century because at that time there were no British or Hannoverian troops around. The Austrians were the only ones left to oppose the expansion of France on the continent after the peace treaty of Basel in 1795. The British were still in the war but they did not participate in the fighting that was going on in Germany, nor did the Hannoverians [17, p. 406].

In the middle of the 18th century the situation was completely different. During the War of the Austrian Succession, lasting from 1742 until 1748, British and Hannoverian troops played an important role in the war against France on German soil; see for instance [20]. The same can be said about the Seven Years War, that lasted from 1756 until 1763 [18]. Probably the origin of our letter goes back to one of these wars, which of course would make the elder König its author. The next step is to find data that link both the British and the French more closely to Camberg.

Let us first single out the Seven Years War. There was fierce fighting between the British and the French on the Nassau-Dillenburg territory during the years 1759 and 1760. As a matter of fact, the old ancestral castle of the House of Orange, the Dillenburg, was first occupied by a Hannoverian garrison and thereafter by a French one. In the course of the hostilities it was fully destroyed never to be built again [12, p. 139; 18, p. 174–188]. The fighting however was concentrated on the northern Lahn region and the area directly surrounding Dillenburg Castle, also more to the north. The French withdrew temporarily to the southern Lahn after the battle of Minden had not gone well for them. This took place in September 1759. They stayed in the southern Lahn region with 54,000 men until November 5th, when a new British and Hannoverian advance forced them to withdraw to Camberg, somewhat more south [16, p. 470]. The advance did not hold and on November 11th the French were back in Limburg, preparing for a new attack on Dillenburg and its surroundings [18, p. 189–198].

It is therefore not fully excluded that our message dates back to that year but the phrasing seems to indicate a different direction. In the message one can find the statement "the French are leaving Camberg but others take their place." This suggests some wavelike movement of troops, as if the French are flooding the country. In November 1759 this is not at all the case. The French withdrawal to Camberg was a more or less unique event. Fighting was concentrated in the area around Dillenburg more to the north, with the line of defence alongside the river Lahn as its most southern theatre. Camberg comes into the picture only once, and only haphazardly.

But there is a second reason why the message is not likely to have been written in the year 1759. At the time, Prince William V was only eleven years old. His father had already died in 1751 and his mother, Princess Anne, died in January

1759, about 10 months before the letter could have been written. It could only have been directed to Prince Louis of Brunswick, the guardian of the young Stadtholder. He had every reason not to take much interest in the well-being of the German principality of his pupil. His primary concern being to keep the Dutch Republic, whose territory had already been violated frequently, out of the war. It made perfect sense to separate affairs in Germany from those concerning the Republic [3, p. 496; 4, p. 159–161].

This leaves the last possibility, that the letter was written during the war of the Austrian Succession, lasting from 1742 to 1748. Mr. König entered the service of the House of Orange in 1744, so in this respect, it could have been written in that year. This would make Prince William IV the receiver of the message. It would mean that at some point in time the letter was filed in the wrong place, not surprising since it was not easy to read! Moreover, William IV is a far more likely candidate for having received the letter than his son. In 1739 the principality of Nassau-Dillenburg was reunified after having been divided into four parts for many years. The reunification was caused by the extinction of a side branch of the ruling family and it marked the beginning of a reorganisation of the government under the direct supervision of the Prince [12, p. 98-100]. William IV visited his principality regularly and while staying in the Republic, he was kept informed by means of his own courier service.[11]

The war of Austrian Succession brought much diplomatic manoeuvring. The Prince was married to an English princess and therefore tended to side with the Austrians or rather the 'pragmatic alliance' as the countries were called, wanting to uphold the rights of Maria Theresia, daughter of the last Habsburg emperor.[12] But he was a personal friend of Frederick the Great of Prussia too. Moreover, the French were never far away and he needed the support of the newly elected emperor (who was backed by the French) to get confirmation for his claims on his newly acquired territories [9, p. 91; 12, p. 98-100]. As a matter of fact, in 1743 (shortly before the Battle of Dettingen) the British did send a small army to Nassau, to prevent the Prince of Orange from getting too close to the French and their Bavarian puppet on the imperial throne [8, p. 88]. They were stationed, among other places, in Camberg and they were welcomed by the Prince who

[11] This can be derived from his correspondence with the governor of Nassau-Dillenburg, C. H. von der Lühe. See: Koninklijk Huisarchief, stadhouder Willem IV, inv. nr. 351. The courier or "estafette" is mentioned in a letter from 1745, september 18th in which he announces a forthcoming visit to his german principality.

[12] The letter mentioned in the previous footnote gives detailed instructions for the preparation of a meeting with Maria Theresia on the occasion of the crowning of her husband as German emperor in Frankfurt. The empress had to understand that the support she received from the British side was largely due to William's interference! For his marriage to a daughter of George II see: [9, p. 20–28].

even applied for an office in the British army.[13]

This would account for the British but were there any French? At the time there were not, but from December 1744 onwards they were present; at least in the area [15, p. 485–486]. At the end of March 1745, the French commander of the Rhine army, Maillebois, concentrated most of his army here and even stationed his headquarters at Camberg, in order to prepare an attack on the area north of the Lahn. Hannoverian troops had already evacuated the area south of the river Lahn on March 16th but they had left allied garrisons at Diez, Limburg and at Ober- and Nieder Lahnstein, where the Lahn flows into the Rhine. These troops were withdrawn about two weeks later, respectively from Diez and Limburg on April 10th and 11th, and from the mouth of the Lahn on april 14th [15, p. 480, 494–495].

From this moment on, French troops were concentrated alongside the Lahn but fresh replacements were brought in to occupy the territory they left behind, most notably Camberg. The objective was to ensure that the allied forces north of the Lahn could not contact those in the south of Germany [15, p. 496–500]. The requisitioning lists informing us about the presence of the British troops give details relating to French troops too. They stayed in Camberg the last week of March and the first half of April and possibly longer because requisitioning continued to take place until the third week of May. The first wave consisted of infanterymen, dragoons from Limoges and some hussars, commanded by a Mr. de Biac; the second wave came in on March 30th, stayed until April 12th and consisted of regiments from Montboissier and Monaco, commanded by a Mr. d'Arnault. The men from Monaco stayed until the 17th. From April 20th until April 26th unspecified troops under Marquis de Bouzols are mentioned; this could refer to a third wave.

There are no records of captured stocks of beer but the French were short in supplies and the recurrent flooding of the Camberg area by troops is all too obvious to ignore [15, p. 494].

It seems highly probable, therefore, that our message can be dated somewhere during the month of April 1745.

REFERENCES

1. Allen, E. J. B. 1972. *Post and Courier Service in the Diplomacy of Early Modern Europe*. Den Haag, Netherlands: Martinus Nijhoff.

[13] Hessisches Hauptstaatsarchiv, Akt Abt. 356 VII 19. British presence in Camberg lasted from April until June 1743. It concerned grenediers, respectively from the first, second and third divisions. In May, dragoons from the "Hongward" regiment were present too. In June they were joined by Hannoverian troops.

2. Benschop, W. J. M. 1943. Secrete regeringszorg met medewerking van het Haagsche postkantoor (1752-1795). *Bijdragen voor Vaderlandsche Geschiedenis en Oudheidkunde* VIII(4): 238–260.

3. Bootsma, N. A. 1962. *De hertog van Brunswijk, 1750-1759*. Assen, Netherlands: Van Gorcum.

4. Carter, A. C. 1971. *The Dutch Republic in the Seven Years War*. London: Macmillan.

5. Colenbrander, H. T., ed. 1912. *Dépêches van Thulemeyer, V–XXII*. Amsterdam: Johannes Müller.

6. Fain. 1926. *Neun Jahre Napoleon's Sekretär 1806–1815*. Berlin: Ernst Klarwill.

7. Fleissner von Wostrowitz, E.B. 1881. *Handbuch der Kryptographie*. Wien: Seidel & Sohn.

8. Fortescue, J. W. 1899. *A History of the British Army. Vol. II*. London: Macmillan.

9. Geyl, P. 1924. *Willem IV en Engeland*. Den Haag, Netherlands: Martinus Nijhoff.

10. Heck, R. 1908. *Die Drangsale der Stadt Dietz während der Revolutions Kriege*. Dietz, Germany: Meckel.

11. Hindenburg, C. F. 1796. *Archiv der reinen und angewandten Mathematik*. III: 347–351, V: 81–99.

12. Japikse, N. 1938. *Geschiedenis van het Huis Oranje-Nassau*. Den Haag, Netherlands: Zuid-Hollandsche Uitgevers Maatschappij.

13. Kahn, D. 1967. *The Codebreakers*. New York: Macmillan.

14. Leeuw, K. and van der Meer, H. 1993. "A Homophonic Substitution in the Archives of the Last Great Pensionary of Holland." *Cryptologia*. XVII(3): 225–236.

15. Pajol. 1883. *Les Guerres sous Louis XV. Vol. II*. Paris: Librairie de Firmin-Didot et Cie.

16. Pajol. 1885. *Les Guerres sous Louis XV. Vol. IV*. Paris: Librairie de Firmin-Didot et Cie.

17. Palmer, R. R. and Colton, J. 1971. *A History of the Modern World*. New York: Alfred A. Knopf.

18. Savory, R. H. 1966. *His Britannic Majesty's Army in Germany during the Seven Years War*. Oxford: Clarendon Press.

19. Schama, S. 1977. *Patriots and Liberators*. New York: Alfred Knopf.

20. Skrine, F. H. 1906. *Fontenoy and Great Britain's Share of the War of the Austrian Succession 1741–1748*. Edinburgh and London: William Blackwoods and sons.

21. van Seeters, W. H. 1962. *Pierre Lyonet.* Den Haag, Netherlands: Martinus Nijhoff.

22. Weniger. 1899. *Geschichte des Schlosses Oranienstein.* Dietz, Germany: Meckel.

BIOGRAPHICAL SKETCHES

Karl de Leeuw is a historian. He is currently involved in a project of surveying Dutch archives for the occurrence of cryptographic material relevant to the history of the Netherlands as an independent state, since the end of the sixteenth century.

Hans van der Meer is working at the University of Amsterdam in the faculty of Mathematics and Computer Science as a teacher of computer science, cryptography, and computer security.

ENEMY CODES AND THEIR SOLUTION

FROM THE ARCHIVES

Editor's Note. During the course of their research, our editors and readers are sometimes responsible for the declassification of previously undisclosed material. Or they may discover items in private or public collections, libraries, and archives, items which are not widely known. The purpose of this column is to give these documents wider circulation for the benefit of the cryptologic community. If you have or know about material suitable for this column, please send it to David Kahn, 120 Wooleys Lane, Great Neck NY 11023 USA. All contributions used will credit the donor.

The following pamphlet was discovered by David Kahn in the United Kingdom's Public Record Office, London under file number ADM 137/4659.

Enemy Codes and Their Solution, published by Intelligence (E), Ciphers, General Headquarters [British Expeditionary Force], January 1918. In the original it runs 52 pages. Appendices 3 and 9 are the only ones given. No author is listed.[1] The study was obviously intended to teach fledgling cryptanalysts how to solve German field codes, which were at the time or publication the chief form of front-line cryptography. Studies of code cryptanalysis are rare in the literature of cryptology, and the reprinting of this one seeks to help fill that gap.

David Kahn

[1]Though perhaps it was written by or under the supervision of the officer in charge of Intelligence E(C) whose name stands at the foot of Appendix 3, Captain O. T. Hitchings.

INDEX - RENUMBERED FOR THIS EDITION

INTRODUCTION

As the following brochure is primarily intended solely for the purpose of showing the methods adopted in solving the codes used by German Field Wireless Stations, it is not proposed to enter into a long explanation of the nature and solution of codes in general. It is obviously impossible within the limits of a short treatise to treat exhaustively all the aspects of code solution, nevertheless, a few preliminary remarks on the subject may well fall within the particular scope.

DEFINITION OF A CODE

A code is in essence a conventional dictionary used for the purpose of translating, by means of combinations of letters or figures, a secret communication into such a form that it cannot be deciphered by anyone not in the possession of the code book.

In codes used by German Field Stations certain groups of letters are allotted to the words and phrases most frequently used in conveying information of a military character, as well as to numbers and to the most frequently used spelling groups.

A number of groups are also allotted to the various punctuation marks and grammatical signals such as

HAUPTWORT, MEHRZAHL, GEGENWART, MITTELWORT DER VERGANGENHEIT,

and several groups are definitely set aside as dummy groups to be inserted in frequently recurring phrases and in short messages of a more or less stereotyped character.

The advantages of such a system of secret correspondence are obvious. Encoding and decoding are easy and rapid: the encoded message is generally much shorter than the original text; the comparison of one message in code and in clear does not enable another message in the same code to be read; and the measure of security is high if not absolute, unless the code book falls into the enemy's hands, or has been in use for such a long time that a sufficiently large amount of material has been intercepted to enable the enemy to solve it.

QUALIFICATIONS FOR THE WORK

In order to undertake successfully the reduction of a code certain preliminary qualifications are essential. Much time and much labour must be devoted to the work if any useful measure of success is to be obtained.

The would-be solver must possess a thorough knowledge of the language employed, not only from the point of view of vocabulary but also from that of a knowledge of all the peculiarities of its grammar, syntax and idiom, and of the peculiar phraseology, diplomatic, commercial or military, in which the messages are likely to be couched.

He should possess a lively intelligence, the faculty of imagination tempered by a highly developed critical faculty, the power of analysis, a high degree of a certain natural flair or instinct for the work, untiring patience and perseverance, in a word, the qualities of genius, defined as an infinite capacity for taking pains.

He will need a dogged obstinacy, which however must not render him incapable of discarding a supposed clue, once it has been discovered not to lead anywhere; a highly trained visual

memory which will help him to remember the look of a code group, to recognise it on its reappearance, and to remember where he has seen it before, what its sequences were, and what theory, if any, he had formed about it each time it occurred.

He must possess the faculty of keeping anything from a dozen to twenty theories in his mind in order to build up a chain of coincidences and reasoning until each link fits into its place and forms a coherent whole.

IMPORTANCE OF METHOD

In addition to the above qualifications, however, a right method, and a clearly defined system of attack on a new code are necessary. It is the purpose of this brochure to try and lay down the main principles of a logical method, such as enabled the first code to be solved without the aid of previous analogies, and the more or less adventitious assistance of a knowledge of all the peculiarities of phraseology and procedure adopted by certain stations or groups of stations.

At the same time, however, as much reference as possible will be made to all analogies which may lead to a successful attack on a new code when its general outlines, scope and procedure are known.

FIRST STEPS

At this stage a tabulated summary of the most essential steps to be taken will perhaps be most useful. Later on a more detailed elaboration of these steps will be brought in under the various sections as they occur.

1) The first step to be taken is to collect all the material that has been accumulated and have it typed out in such a way that the maximum amount of material can be brought under the eye at any one moment.

The material should be sorted as far as possible into sections showing the sender and receiver, and keeping as close together as possible all messages from the same station or group of stations.

Any indication in clear at the beginning or end of messages should be shown, such as sender, receiver, time group of transmission, Chi or Zif numbers showing the numbers of groups etc.

All pages should be numbered consecutively, and each separate message on a sheet should be given a serial letter. This will enable reference to be made to any particular code group or message by giving the number of the page and the letter of the message, i.e. 21B, 36K, etc.etc.

2) A book should now be prepared in which the letter or figure groups can be arranged in order, after which every group that occurs in the code should be indexed in the book by giving its reference as above.

In proportion as the signification of any group is discovered, its indexing should cease, and the meaning should be inserted opposite to it on the line. A sample page of such an index is shown in Appendix (2).

This book will then serve as a decoding of "Entzifferung" book as well as an index. It will be well at the same time to mark the initial and final groups of each message in some

distinctive colouring on the index, so as to facilitate the study of these particular groups, and to aid hypothesis as to their function when they should be frequent.

3) The index will soon begin to show the frequency of the recurrence of the various groups employed.

Attention should be concentrated on the initial and final groups which might indicate the address or signature respectively, or the word "an" "addressed to" or "intended for".

If the sequence of the first two groups should show any tendency to be at all constant it will be extremely probable that the first = "an", and the second = "unit" or person addressed.

Any outside knowledge as to the nature of the possible unit, or the rank, designation or name of the possible person may well aid hypothesis at this stage.

Very soon it should be possible to identify the various groups for "Division", "Brigade", "Regiment", "Kampf-Truppen-Kommandeur", "Funken-Telegraphie-Station" etc.etc.

When the study of numbers, treated in detail elsewhere, has resulted in identifying the groups which must be numbers, although as yet their actual value is not known, we have now reached a very fruitful stage for hypothesis as to the numbers of the possible units mentioned.

INITIAL AND FINAL GROUPS

4) An analysis of the most frequent final groups in each message should now lead to the discovery of signatures, of Punkt = Full stop, or of Fragezeichen = Note of interregation. The last mentioned is very frequent in short messages such as "Wo bleibt Abend Meldung?" or "Wie ist die Lage dort?" etc.etc.

A comparison of initial and final groups will now often show that the same group occurs at the beginning of some messages and at the end of others. This will point fairly conclusively to the fact that these groups represent the units or person sending or receiving the message.

Any outside indication as to the possible sender and receiver in each case will now be useful in forming an hypothesis as to the signification of these address and signature groups.

At this stage, as in fact at nearly every other, analogy with previous messages sent by the same station in codes already known or solved should be studied as far as possible.

A knowledge of the possible subject matter of messages sent at stated times, or under circumstances about which any outside or collateral information can be obtained should always be sought for, and will invariably and inevitably assist in experiment and hypothesis.

INTERIOR GROUPS

5) We now approach the most difficult part of the solution, namely that of the inside portion or text of the message. This it is proposed to undertake by a separate treatment of the several kinds of groups which normally occur in the text of messages.

These may be usefully treated under the general headings of Phrases, words, spelling groups, (used for spelling cut words or names for which there is no equivalent group in the code), punctuation marks and grammatical signs.

Of these, for reasons to be explained later, the numbers are, in the early stages of the code, the most important, and their study shall therefore be treated first.

It must be remembered however, that it is almost impossible to separate one portion of the work of solution from others, and as stated earlier on, the efficient code solver must possess the

faculty of keeping many possibilities and collateral theories in his mind, even while endeavouring to concentrate on some one particular aspect of the work.

The whole problem resolves itself into a coordination of hypotheses, separately obtained by analysis, theory and imagination, but linked together by every possible means until the whole chain of reasoning is found to be complete.

NUMBERS

Importance of numbers

In the days when cipher was employed to the exclusion of code, there was no necessity to concentrate on numbers apart from their context. The key once discovered, the whole message and all succeeding ones were immediately decipherable in their entirety.

Now however that code has taken the place of cipher the verification of numbers assumes a much more important aspect.

As it is obviously impossible to solve the two thousand odd groups which exist in a code until they have been used in messages, or even then until some of them have occurred sufficiently often to enable one to analyse their sequences and positions, the code has to be built up little by little, in proportion as material comes to hand.

It becomes necessary therefore to concentrate on what will be most immediately useful, and one of the most important pieces of information that we can obtain from enemy wireless messages is the identification of units in the German lines on any particular portion of the front, for the purpose of ascertaining what is the strength of the enemy forces opposite to our own.

For this reason we will begin with the solution of numbers, and consider this problem from the double standpoint of solution by analogy and solution on first principles, combining the two methods whenever the necessary progress has been made.

An essential preliminary is a knowledge as complete and detailed as possible of the constitution of the German Army and of the German order of Battle.

I. SOLUTION BY ANALOGY

In these codes numbers are used in the following ways;-

a) In mentioning Units, Divisions, Brigades, Regiments, etc.

b) In mentioning dates and times of day.

c) In giving map references after Karten Punkt and Planquadrat.

d) In giving numbers of shots, casualties, Funken-Telegraphie-Station accessories.

e) Number of messages sent and received,
e.g. "3 Funksprueche geschickt, 4 empfangen."

f) In giving tabulated reports of the days activity under various headings.

g) Chi or Zif numbers and time of groups of messages answered or referred to,

e.g. "Chi 17 an KS night verstanden"

"Funkspruch 1306 erledigt"

"Wer hat Funkspruch 1037 gegeben ?" etc.etc.

A sample message including most of the above uses might run as follows;-

"An Division 105. Abend Meldung 18-2-17. (1) Von 10 Uhr 25 Morgens bis 3 Uhr 30 Nachmittags 40 Schuesse schweren Kalibers auf Kartenpunkt M2 Planquadrat 5209. (2) Feindliche Flieger Taetigkeit gering, 5 Flieger ueber Abschnitt 7A. (3) Wetter gut, sicht klar. (4 bis 7) nichts. (8) 2 Unter-Offiziere und 7 Mann schwer verwundet, 10 Mann leicht verwundet. (9 bis 10) nichts. Gezeichnet Bataillon II / 316."

The form of these report messages varies with each sector and group of stations, but the same station has the tendency to send the same form of stereotyped message at certain stated times each day, and a careful analysis of previous messages from the same station in an old code will often be of material assistance in solving a new code.

One of the most essential things therefore in starting to solve a new code is to study as carefully as possible all previous messages, with reference to matter, form, and station procedure with all its varying peculiarities, and to analyse and experiment on the new messages to find out any analogies which may exist.

It has often been possible to make a start on a very limited amount of material when the same stereotyped form of message is still being transmitted by the same station.

It frequently happens however, that with a change of code or a change of unit, these messages are no longer sent in the same stereotyped form. Some messages rarely mention units, others rarely give the date, and some use letters instead of numbers in sending tabulated reports.

In one code certain stations regularly sent messages of this type,

"2 geschickt, 5 empfangen.",

but with a change of code such messages ceased altogether.

In the same code one station regularly sent a message in the following form ;-

"Regiment b' Abend Meldung b' (1) etc."
"Regiment b' Morgen Meldung b' (1) etc."

with a tabulated report on stereotyped lines.

When the code changed the form of these reports changed absolutely and no analogy could be observed. These changes were most possibly due to the transference of the particular Difua to another sector of the front.

When the form of procedure thus changes and analogy breaks down we are thrown back on solution by first principles, just as when the first code was solved without the help of previous knowledge of station procedure and phraseology.

II. SOLUTION BY FIRST PRINCIPLES

In solving a code without the aid of analogy there is a tremendous amount of preliminary spade work to be done

a) by indexing,

b) by analysis of frequent groups and their sequences,

c) by a study of what may be called in a general way stationary groups, i.e. Punkt, Uhr, An, Von, Bis, Meldung, etc., and mobile groups, i.e. numbers, spelling groups and words,

d) by a search for groups which have a tendency to recur in pairs.

These are explained more fully elsewhere.

In earlier codes the problem was rendered much easier by the fact that there was only one group for Punkt, Komma, Uhr, etc., and by the fact that each number up to nine was represented by only one group.

This meant that to encode compound numbers such as 15, 25, or 105, the single numbers were used, and to encode 17th or 21st the single cardinals were written followed by "te" or "st" etc.

In the present codes unfortunately the tendency has been to increase the number of groups for each cardinal up to 10, to give groups for compound numbers from 11 to 20, and 20 to 100, and to allot groups to all ordinals up to 12th, and to frequentatives from "einmal" to "zehnmal".

But in spite of these increased difficulties it is possible to lay down a certain number of first principles such as may help in elucidating numbers.

As numbers tend to be some of the most frequent groups apart from Satzzeichen, the preliminary spade work should have resulted in spotting certain frequent groups.

By marking these groups in distinctive colours as shown in Appendix (1) it will be noticed that some of them have a tendency to attract each other, and to hunt in couples, threes, and occasionally fours.

Now groups which invariably appear in couples, in the same order, will most probably be nouns or verbs followed by "Mehrzahl" or "Mittelwort der Vergangenheit" etc., station calls, or stereotyped phrases such as "Morgen Meldung", "Abend Meldung", "KTK A" or "KTK 3" etc.

Groups which invariably run in threes or fours, or more, in the same order, will most probably be spelling groups, and might give P- O- ST, L- AM- P- E, S- A- TZ- B- U- CH, etc.

But when groups tend to appear generally in bunches of two, three of four, and not always in the same order, most if not all of them will turn out to be numbers.

Thus if A, B, C, D, E, F should represent half a dozen of these frequent groups they might occur in the following orders;- A B or B A; A C E, E A C, or E C A; B A D C or E A B D etc. It will then be safe to presume that these groups represent numbers.

By tabulating the sequences before and after any one of these groups they will soon be seen to attract others, until anything from 12 to 20 of them can safely be presumed to be either numbers or some word or letters which frequently accompany numbers, such as Unit, Uhr, Komma, Planquadrat, von, bis, zwischen, und etc., or one of the letters of a station call such as K 3, 9 D, M 4, etc.

Bearing in mind at this stage what was said above about stationary and mobile groups, it should now be possible to discover that some one frequent group, not a number, frequently precedes two or three mobile groups, and might be Division, Brigade or Regiment, or comes always second or third in the sequence, when it might be Uhr or Komma used instead of Uhr.

If the presumption is in favour of the stationary group being Uhr, a tabulation should now be made of all the groups preceding and following it, going for instance four backwards and four onwards in each case, and keeping the stationary group always in the same perpendicular column. This is shown in Appendix (1b).

If the presumption in favour of Uhr should be correct, this group should practically invariably be preceded by and most frequently followed by one or two numbers although as yet the latter may remain unidentified.

It should now be possible to discover von, bis, zwischen and und, bearing in mind the usual formula as shown in the sample message above.

This is best done by concentrating on the most frequent group (not obviously a number) which almost invariably precedes the one or two mobile groups (numbers) followed by the stationary group (Uhr). If there is any such frequent group it should be "bis". The discovery of "von" follows logically.

As certain Satzzeichen such as Punkt, Komma, or Bindestrich, and certain frequent words such as "und" and "von", occur often in close proximity to numbers, it is well at this stage to try and separate these groups from those representing numbers. This is best done by the system of distinctive marks, as explained above.

When the groups coloured in a distinctive way tend to occur in other parts of the messages away from numbers, and in certain more or less easily recognisable positions, they are probably not numbers themselves.

For instance "Punkt" will occur frequently at various parts of messages and often at the end; "und" will of course appear in many places where none of the presumable numbers are around it.

Punkt, Komma and "und" moreover will not have appeared immediately *before* the Uhr which has been analysed and its recurrences and sequences tabulated.

By proceeding on these lines it becomes possible to sort out many groups which though they have a tendency to go with numbers are not numbers themselves.

Having now arrived at the stage where we are practically certain of having discovered several groups which must be numbers, there are two or three ways in which it will soon be possible to allot values to them.

It is very useful at this stage to colour or underline distinctively all presumable numbers, not necessarily in different ways, but by giving a uniform mark to distinguish it as a number.

It will then be possible to concentrate on any agglomeration of numbers which occurs at the beginning or at the end of messages.

This should result in identifying the groups representing units, especially if a careful analysis of all initial groups of messages has resulted in a presumable "an".

By studying the daily Intelligence E (c) summary (cf. Appendix 3) to see what units are connected with the station concerned, it will be possible to conjecture numbers of Divisions, Brigades, or Regiments.

By comparing one conjecture with another and noticing points of similarity, it will soon be easy to give definite values to the numbers of units. This is done in the following manner.

If one address or signature should be in the order X.Z.Y., and another in the order V.Y.W., and if there were Regiments connected with those stations with the numbers 245 and 356 respectively, this would easily lead not only to the conjecture that the group Y=5, but also that X=2, Z=4, V=3 and W=6. It might then be possible to find an address

"an (Unit) X.W."

which might quite well fit as Brigade 26 in the sector concerned.

By a system of check and cross-check on these lines many numbers will be identified.

Having got so far it will now be well to concentrate for a time on the numbers before and after "Uhr". Here certain definite assumptions may be made.

The numbers preceding Uhr must range from 1 to 12. If by good fortune there are two numbers in front of Uhr, the first must be *one* and the second 0, 1 or 2.

This was very easy to ascertain in the former series of codes, but unfortunately in the recent ones the compound numbers 10, 11 and 12 are practically invariably used.

If there is only one number after Uhr this will practically certainly be 5, 10, 15, 20, 30, 40, or 50. Of these by far the most frequent is 30. When there are two numbers after Uhr the first will range from 0 to 5, and the second will almost invariably be 5.

These hypotheses may now help the checking and cross-checking of unit numbers, and may lead to more identifications.

At this stage much valuable assistance will result from an analysis of all messages containing "von – bis –". Here the second number will obviously be higher than the first, except in such a case as

"von 9 Uhr 15 bis 9 Uhr 45"

when it will have the same value.

There are other frequent uses of "bis" besides those in connection with times of day

i.e. "20 bis 30 Schuesse"

"5 bis 8 nichts "(in tabulated reports)

"vom 4ten Abends bis 5ten Morgens"

which however are now almost invariably ordinal numerals, etc.

There are other clues which may lead to the comparative size of a number. A very frequent request is as follows ;-

"Sofort einen Mann nach KW schicken."

Here the number is nearly always "eins".

In asking for wireless apparatus and accessories one of the most frequent messages is

"Bitte ( ) Akkumulatoren"

where the number is always relatively low, 1, 2 or 3.

In reporting the number of messages sent and received in the form

"- - geschickt, - - empfangen"

the numbers are also relatively low, ranging generally between 1 and 8.

In the case of a message which mentions a Chi or Zif number, or the time-group which is always prefixed to each message, it is often possible to discover the message referred to.

For instance in a message from KS to MD, we might discover a group of four numbers, obviously referring to the time group.

Example;-"Funkspruch - - - - ohne Sinn"

By referring to previous messages on the same day, we find one from the same station timed 1309. The presumption is very strong that these are the four numbers referred to, and if we have already identified two or three of these numbers we can now determine the value of the remainder.

A still more satisfactory discovery is that of a serial report, such as the one quoted above, where the numbers will obviously be consecutive, and will sometimes give the whole series from 1 to 10.

Occasionally numbers can be identified by their inclusion in spelling groups. Of such numbers "ein" is by far the most frequent, the group for this syllable frequently serving the double purpose of spelling group and the number "eins".

More rarely we have examples such as

"2 Mann RE - VIER krank."

"Erhoehte Funken-Telegraphie Bereitschaft, gut acht geben"

"Es besteht zwei - F E L darueber."

METEOROLOGICAL REPORTS

Meteorological reports are often extremely useful in assigning values to numbers previously unidentified. A characteristic code message would run;-

> "Wetter Meldung von 26 - 12 - 17. Boden Wind hundert, null, sechs; zwei hundert, null, acht, fuenf; hundert, null, zwoelf; eins, fuenf, null, null; Barometer 03,6. Temperatur minus 3 ; 6. Feuchtigkeit 92 prozent. Luft gewicht 171,30."

GERMAN WIRELESS PRESS

Another fairly frequent type of message is an extract from the wireless press dealing with number of prisoners and guns captured in some theatre of war. For instance at the time of the Italian débâcle we frequently had code messages of the following types;-

i) "A und B Kompagnie. Hundert achtzig tausend Gefangenen, hundert Geschuetze; an einem Tage sechzig tausend Mann und vier hundert Geschuetze. Gemona ist gefallen."

ii) "Gefangenen Zahl am Isonzo erhoehte sich auf sechzig tausend und 450 Geschuetze."

A study of our own meteorological reports for the same date and time, and a study of the day's German wireless press will be very useful. By comparing the code message with the clear it will often be possible to see exactly what the right translation should be.

REPORTS ON FLOODED AREAS

One of the most interesting and at the same time useful type of message is one which appears twice daily on the flooded sector of the Yser. By opening the dams at certain places the Germans are able to flood certain districts.

At the above stated times each day a certain station sends a code message dealing with the height of the water above and below the dam in question.

As these messages are very stereotyped in form they are extraordinarily useful in identifying numbers far more quickly than would have been otherwise possible.

A typical example runs;-

> "1ste Reserve Pioniere 13. Wasserstand 6 Uhr Abend OB-ER-STROM 4; UNTER-STROM 3,65 Meter."

These things are of course only adventitious aids to the solution of a code, and are of most use when the solution has already reached a certain stage, i.e. when some of the more frequent spelling groups and words have been identified.

By continual analysis, hypothesis and experiment on all the above lines, employing analogy where available and first principles when that fails, leaving no stone unturned, and pursuing a perpetual system of check and cross-check, we at length reach the satisfactory stage of verifying all the numbers.

This is obviously a much more difficult task than in the previous series of codes, where it was only necessary to identify one group for each number, but even with the current series the problem is not incapable of solution.

WORDS AND PHRASES

By the time that numbers have been identified, or at any rate a certain proportion of them, many odd words will have been discovered simultaneously. Of these the most probable discoveries will have been von, bis, zwischen, und, Uhr, times of day, and possibly more or less definitely fixed values of the various synonymous expressions for Schuss, Flieger, Akkumulator, etc.

Having arrived at this stage, further hypothesis becomes more easily possible, and we may be gratified by a leap forward in the solution, and a considerable number of obvious identifications for groups will occur to us.

It is at this stage however that it is necessary to make haste slowly, as there is always a tendency to assume that a certain group must have a certain meaning because of its context in one particular message.

It is here that the critical faculty should step in, and this should be aided by the use of the index which has been made. Before asserting that the meaning of a group is such as we presume it to be on the one example, it is absolutely essential to find all its references in the index, and to assure ourselves that the presumed meaning will fit in all the places in which the group occurs.

Having proved this by at least four or five occurrences we may then find that the group in question occurs in messages where none of the surrounding groups are as yet identified. When this is so it forms the basis of conjecture as to the probable meaning of the groups before and after it.

For this reason whenever the meaning has been proved without a shadow of a doubt it should be written over the group wherever it occurs, and all the surrounding groups should be exhaustively analysed.

The best and safest method of doing this is to write the group in question on a separate sheet, and to write out its sequences, going backwards and forwards for at least four groups. When the meaning of any of the surrounding groups is determined, the translation of them should be given.

The same process should be gone through with any group that is being experimented on. It will then frequently become possible to form a chain of reasoning so secure that we can safely assume the meaning of the group to be correct on only one occurrence instead of having to wait for its repetition several times to assure ourselves of its correctness.

The basis of reasoning becomes almost Euclidean or algebraical, i.e.

If A = Z, then B should = Y; if B = Y, C should = X,

If C = X, we may by this time be fortunate to find a sentence in which the whole chain is found to be sound and the sentence will read coherently.

It is at this stage of solution that the faculty mentioned above of being able to keep a dozen or twenty groups in one's mind at a time, with their sequences and context whenever known, and any theories that may have been formed about them when first encountered, will be most invaluable.

It is obviously impossible to treat this process at all fully without taking a score or two of pages in a code, and reconstructing all the mental processes, all the hypotheses, and all the clues, fruitful or otherwise, which have led to the complete reduction of the code.

A few examples may however serve to illustrate the meaning of what has been said above. When a sufficient number of spelling groups had been identified in one particular code to spell out V I Z E — W E D E L, very little additional evidence was necessary to supply the missing group "Feld".

In previous messages a certain group by its position and possible function in the sentence partly decipherable seemed to be a preposition.

By inserting the word "Feld" wherever its equivalent group occurred, it was found in one or two instances to follow the above preposition.

In another case this same preposition preceded a time of day. The assumption was very strong therefore that the preposition was "vor", giving "Vorfeld" in one case, and "Vor acht Uhr Abends" in the other.

In another case it came followed by "und". This led to the assumption that the group after "und" was "hinter". The assumption proving correct led to the discovery of "Vor-und Hinter-Gelsende", which fitted in excellently with a patrol report, and led on by successive steps to more and more identifications.

Returning once more to the group for "Feld", it was seen to occur after two unknown groups, where it might be part of a place name or of the territorial designation of a unit.

The two unknown groups referred to, (let us call them X & Y) were also discovered close together in a sequence of groups as follows;- (W) L U E - (X) W IE (Y), where W= another group previously unidentified.

By comparing the two messages we discovered without undue difficulty that the last mentioned sequence spelt out

SCH-LUE-SS-EL SCH-IE-BER

i.e., a sliding alphabet ruler, and that the place name was EL-BHR=FELD. By inserting with the aid of the index the identifications SCH, SS, EL and BER wherever their groups occurred many more spelling groups were discovered and these in their turn led to others, until most of the spelling groups were discovered.

SPELLING GROUPS

At this stage it is necessary to discuss the use of spelling groups and to know how their solution may be obtained.

In the initial stages of the solution of the codes used by German Field Wireless Stations we were absolutely in the dark as to the nature and extent of the employment of spelling groups.

In many codes, when it is necessary to spell out a word for which there is no equivalent in the code, the custom is to employ spelling groups solely for individual letters.

This means that when the characteristic recurrences and sequences of simple substitution occur, the presumption is that spelling groups are being employed.

By applying the principle of the solution of simple substitution to the particular parts of the messages where these peculiarities are noted it is a fairly simple matter to discover the groups used for individual letters.

This is especially the case when any outside knowledge of the probable subject matter of the message, or of the names of persons or places likely to be mentioned, is obtainable.

It would for instance, be fairly simple to spot the translation of the sequence X Q V P Q V (where these letters stand for the code groups employed), as L O N D O N, of W B Z Z B D L B as C A R R A N Z A, of L J C F Q C F M as T H O U R O U T, of X Q S S Y A Y Z Y as Z O N N E B E K E, of M D Q Q H Y A D Q Q M I Q Y Z as D R O O G E B R O O D H O E K, etc.etc., if these names were likely to be referred to in the text.

As in many codes it is customary to insert a "Buchstabier-Gruppe" i.e. "spelling begins", "spelling ends", before and after a word spelt out, it is frequently possible to identify this group by the period of its recurrence, and when once discovered it leads in its turn to the knowledge that the groups within its two repetitions are spelling groups, even if it is impossible at an early stage to identify their exact meaning.

In the code under consideration there are certain frequent words or abbreviations spelt out. Among these the most frequent of the easily identifiable ones are the abbreviations K-T-K = Kampf Truppen Kommandeur, and R-I-R = Reserve Infanterie Regiment.

They sometimes occur with a Punkt or Bindestrich between them, and sometimes without any separating group.

In the early stages of experiment on these codes, one of the things which led to the eventual solution of the code was the very frequent repetition of a sequence of groups which ran as follows;- BS WK RJ WK BS. Variations of this procedure were noted such as BS RJ BS alone; WK BS WK RJ WK BS WK, etc.

Before noticing these various peculiarities the tendency was, on the analogy of simple substitution, to imagine that the first form mentioned above was such a word as N E U E N, N E B E N, S T E T S, etc., but when, later on, the second and third variations were discovered,

it eventually became evident that the WK = Punkt or Bindestrich, and that the BS RJ BS = either R-I-R or K-T-K.

This was apparently a very slender thread with which to unravel a whole code, but in codes it must be remembered that "c'est le premier pas qui coûte", and upon this slender foundation the whole code was eventually reconstructed.

In the code under consideration there were groups for spelling far in excess of the 26 single letters of the alphabet. There were modified vowels, double consonants, frequent diphthongs such as au, ei, eu, ie etc., and frequent combinations of two, three or even four letters such as BL, GR, SCH, HEIT etc.

This made the problem of solving spelling groups more difficult, and it was not until this fact was realised that further progress was made. There still were however certain characteristics in the sequences of certain groups, which pointed to the fact that they must be spelling groups.

As was seen above there were sequences in the code which might be spelling such words as "neuen", "neben" or "stets" which turned out to be K-T-K with Punkt or Bindestrich interspersed, but having thus obtained a very possible punkt it became possible to block out the messages into groups representing phrases or more or less self-contained sections of the text.

It was mentioned in the section above which dealt with the solution of numbers that when the code was analysed with a view to marking in some distinctive way sequences of groups which occurred very frequently in the same order, but with different groups before and after them, the presumption was in favour of these sequences representing words or names spelt out in full.

It would be too great a stretch of the long arm of coincidence if on different dates, at different times of the day, and from different stations, there should be same repetition of four or five groups which would stand for the same numbers before and after Uhr, or for exactly the same sequence of words in a stereotyped phrase such as for example

"25 Schuesse auf Abschnitt" or

"Waehrend der Abend Stunden Flieger Taetigkeit gering"

Therefore by collecting several of these frequently recurring sequences, analysing and comparing them, and noticing certain clearly defined characteristics, and at the same time conjecturing what some of the most frequently spelt out words or names would be, it became possible to determine the value of a good many spelling groups.

This process was materially aided by the fact that several of the most frequently used spelling groups were also capable of being used as single words, e.g. in, an, ich, ist, es, da, ein, acht, und etc.

As a fair proportion of these were capable of being discovered by other methods, such as by their recurrence in certain definite places in a message such as "an", or by analysis having proved some of them to be numbers such as "ein" and "acht", we were already on the right road to find out some of the single letters and spelling groups.

Such words as ES-T-AM-IN-ET, L-AM-P-E, W-ACHT-ME-IST-ER, FL-AN-DER-N became gradually capable of solution. Having, as explained above, discovered the values of the groups for K and T from K-T-K, we were very soon able to identify such a word as T-A-K-T-I-SCH or more easily still K-O-N-T-A-K-T.

This "premier pas" had started us off on the high road to success, after repeated failures, "culs de sac", and the inevitable preliminary groupings in the dark which characterise the first attempts at code solution.

One of the most interesting words which helped in beginning to get out the spelling words in a new code was a sequence of groups in the order Q W X Q W X W. This turned out to be B A R B A R A, useful as the code name of a certain unit.

The fact that the same word was spelt out in a succeeding message as B-AR-B-AR-A gave us the group for "ar".

Having got a possible "S" in the word P-O-S-T in another part of the code, we were soon able to identify another group as S-A-TZ-B-U-CH. From this point all was plain sailing.

As the tendency in recent codes, however, has been to increase not only the number of groups for single letters, and short words such as "an", "in", "ist" etc., but also to add groups for less frequent spelling groups such as NG, CHT, RS, etc., the difficulty of solving spelling groups on first principles has increased. The difficulty even then is not as great as it might otherwise seem to be, if the analysis is searching and thorough enough.

For instance it is possible to notice that the same sequence of groups sometimes occurs practically identically, but with one group varying in the different sequences.

When it is noticed that of these repetitions of an almost similar sequence two may be in the form

X K K X Q X T

and the third in the form

X K K W Q W T,

the presumption is very strong in favour of the groups represented by X and W being equivalent to the same spelling group or letter.

When a little thought has resulted in this sequence suggesting the word A P P A R A T we not only have definite values for the P, R and T but also the value of two groups representing A.

At this stage it will be as well to repeat what cannot be too frequently insisted on, namely that, when any value is discovered for a particular code group, this value should be immediately transferred to it every time it occurs in the code.

The mere fact that there are a few odd words, spelling groups or letters hanging in the air in a message, will lead to new theories, which can be proved or disproved by reference to their context, and then carry on the chain.

Spelling groups having been shown above to possess certain characteristic sequences when carefully analysed, it is now possible to determine with more or less accuracy what groups are spelling groups, and apply certain principles of frequency to them.

The frequency tables used in solving substitution ciphers will obviously not apply when, as in this particular type of code we are studying, there are groups for compound letters, in addition to those for the single letters.

For example the letter E which is the most frequent letter in most languages will in this code tend to become one of the less frequent groups owing to its forming part of so many spelling groups.

For all single vowels excepting O in this code there are two code groups, and as O only occurs in two words which can be used as syllables, namely "WO" and "SO", and as moreover

it is a fairly frequent letter it should assume importance if analysed among spelling groups.

It eventually becomes possible to discover a relative frequency of initial and final spelling groups, although this can not be done with anything like the mathematical degree of certainty as in cipher. E, EN, ER, ST will be frequent final groups; GE, SCH, ST, ER, BE, VER will be frequent initial groups.

Of single letters at the beginning of words some of the least frequent in cipher, or in spelling in code when only equivalents for single letters are used, will tend to become much more frequent, owing to the fact that their relative infrequency in clearly defined spelling groups causes them to be employed alone.

Thus D, F, K, M, P, W and Z will rise to a much higher rate of frequency among letters than they reach in cipher.

STATION CALLS

In these codes many valuable identifications of single or modified letters may be obtained owing to their use in station calls. Each German Field Wireless Station uses a particular call sign, and this consists generally of two single or modified letters with an occasional number.

Some stations are in the habit of putting these station calls into code, and when dealing with messages from such stations, bi-groups between "Punkts" or at or near the end of messages should be looked for.

A list of call signs of the groups of stations concerned together with that of the adjoining ones should be referred to, and id one letter of a call sign is known the other will be readily found.

Compare the following message with list of calls ;-

> "WO BLEIBEN GEGENWART STATION MELDUNG MEHRZAHL VON PUNKT sj mo PUNKT rt sb PUNKT mo ne UND rt ne PUNKT."

List of calls. BD - NT - KS - MO - FR - SG - FG.

A glance at the above will show an important point, namely that the final group of one bi-group is the same as the initial one of another, e.g.

sj mo mo ne

By consulting the list of calls it will be found that two of them have the same peculiarity

K S S G

From the above sj mo were assumed to be K S and mo ne to be S G. This again gave rt ne as F G which gave a further identification viz. rt sb as F R.

Having now arrived at the stage where a great many spelling groups have been discovered, we are in a position to discover many short words, which are at the same time used as spelling groups, but which if inserted into their respective places wherever they occur as single words, fix a valuable basis for conjecture as to the meaning of their context. Some of these have been mentioned above, but there will be no harm in recapitulating a few of them.

The spelling M-E-IST-ER gave "ist", which is a very valuable word in a sentence. GE-WO-R-DEN gave WO and DEN, both extremely useful single words.

The spelling of P-I-RE-ALLE-R, a place not far from St. Quentin, constantly referred to in artillery reports, verified "alle", which led to the phrase "an alle Stationen".

KOMMA-N-D-O definitely established "Komma" as distinct from Punkt or Bindestrich.

ACHT-UNG proved the conjecture for the number "acht" to be the right one.

Leutnant NEU-MAHN and other proper names ending in "Mahn" eventually helped in the discovery of TOT, VERWUNDET, KRANK etc.

BE-T-H-MAHN-HOHL!WEG established WEG as distinct from GRABEN or STRASSE, and also gave us HOHL.

The average German operator is not very particular about correctness of spelling as shown in the above mis-spelling of the Chancellor's name; some of his mis-spellings, involuntary or jocular, have given us many valuable short words, and at the same time caused us a certain amount of amusement.

A place called Itancourt, near Birealler frequently referred to in connection with artillery reports was spelt out by one sportsman as I-T-AN-C-UHR-T. Uhr also appeared once in UHR-L-AU-B.

B-U-K-O-WIE-N-A gave "wie", which with "ist" and "wo" quoted above, helped in the discovery of Fragezeichen, as we noticed that interrogative sentences nearly always had a characteristic final group which had previously puzzled us.

SCH-MIT for Schmidt was valuable in proving "mit".

TEL-E-F-O-NIE-SCH and even NIE-CHT for "nicht" gave much help.

On the occasion of the promotion of one wireless operator to be a Funker, a comrade at another station sent the message

"ICH GRAD-U-L-IE-RE"

It seemed almost too good to be true that the group between ICH and -ULIERE should be the word "Grad", but this was confirmed by the use of the index, as we discovered that it came in a meteorological message referring to temperature, and also in GRAD-AUS for "gerade aus".

FR-OE-H-LICH-E WEIN-ACHT-EN gave the group for "Wein".

SCHON-EN DANK was also useful in verifying the possible identification for "schon".

The gem of the whole collection however was "E-SS-EN

"E-SS-EN (gegenwart) Abloesung schon da",

which reminded one of the old Latin catch of one's schooldays

"Mea mater est mala sus !"

A more or less complete list of such short words appears in Appendix (4).

It must be remembered, however, that such helps as these only come when a code has begun to reach a fairly advanced stage of solution.

None of these things which seem so simple and help such a lot at a later stage can take the place of a proper method of attacking a new code, and a firm grasp of the general principles of code solution, coupled with a long and exhaustive analysis on the lines laid down above.

Analogies with previous codes, and as much outside information as may be obtainable, must be worked to their utmost extent, but when the nature and structure of a code change,

or when previous station procedure is no longer adhered to, it is necessary to start working on first principles.

As in the course of the preceding treatment of the solution of spelling groups frequent reference has been made to the principles of Simple Substitution Ciphers, code solvers should make themselves familiar with the main principles of the solution of this form of cipher.

It would take up too much space in this pamphlet to discuss at the requisite length the methods adopted in this process, but information on this subject together with examples for practice, will be found in the "Manual of Cryptography".

A few dozen examples worked out, and a study of the tables of frequency of the language used in the code, and of its characteristic sequences, will prove very useful as a preparation for the study of the solution of codes.

HILFS-SIGNALE

In the particular code under consideration there is a recognised procedure in regard to "Hilfs-signale", and the discovery of these is often of great use towards the complete solution of a code.

Some of these have already been referred to, but at this stage a detailed consideration of their nature and use will be of value.

"Hilfs-signale" are grammatical groups placed after certain words to alter their meaning wherever necessary. The most frequent of them are indications of the tense or number in which a verb is intended to be translated, or of the number of a noun.

They will each be treated separately under their various headings, with an example of their respective uses, and the method of discovering them explained wherever necessary.

1) Hauptwort. (Noun) This group is placed after a verb or an adjective when the corresponding noun does not exist in the code.

e.g. "S.O.S ist der drahtlose anrufen (Hauptwort) (i.e. Anruf) eines Schiffes das sich in groesster Gefahr befindet."

"Welche Wellen-lang (Hauptwort) (i.e. Laenge) gebraucht die Station?"

The context is often sufficient to determine the function of this group. Inserted at each recurrence by the aid of the index, it is often very useful in conjecturing the actual meaning of the preceding group, hitherto unidentified.

2) Einzahl. (Singular) This is used to indicate the singular of a noun, of which only the plural form exists in the code. i.e. after "Korzen", (inserted in the code in the plural because of its frequent use in speaking of candle power) or after "Kontrollschuesse", "gelbe Leuchtkugeln", "Granaten" etc., of which only the plural form is given.

It is also used after verbs to indicate the use of the singular number, i.e. "Wo bleiben (Mehrzahl) Abend Meldung?" and even occasionally to convert a verb into a noun, i.e. "Hoihen folgen (Einzahl)" "Reihenfelge."

3) Mehrzahl. (Plural). This is one of the most frequently used grammatical groups. It indicates the plural number of a noun referred to, and is very frequent after Schuss, Kompagnie,

Akkumulator, Funkspruch, Graben, Flieger etc.etc.

Example, "30 Schuss (Mehrzahl) auf Graben (Mehrzahl) westlich von (Place name)"

Owing to the frequency of this symbol it can often be very easily discovered. When beginning to analyse a code, all groups which have a tendency to occur in pairs should be specially marked, and the two groups bracketed together. It will then be found that one of them is invariably the second one of the bi-group.

When this second group occurs frequently as the second member of several bi-groups it will frequently turn out to be "Mehrzahl". Conjecture as to this may be facilitated by a consideration of the position of these bi-groups in the message.

This often helps to discriminate it from "Mittelwort der Vergangenheit" (past participle) which is also a very frequent "Hilfs-signal".

As it is exceedingly useful in guessing the meaning of a whole sentence to know that a certain group is either a noun or a verb, any group which has the newly discovered "Mehrzahl" after it, should be bracketed to it, and should be noted as a noun.

This noun, although as yet unidentified, should be noted as such, by the aid of the index, every time it occurs even when not accompanied by the plural sign.

4) EIGENSCHAFTSWORT. (Adjective). This is comparatively rarely used, but many serve to turn a word which only occurs as a noun in a code book into an adjective. When discovered, its occurrence should be similarly noted, as for "Mehrzahl".

5) 1 ste Steigerungs form. (Comparative)
2 te " " (Superlative)

These two symbols, as their name implies give the degree of a comparison in which an adjective is to be translated.

e.g. "Feindliche Artillerie Tastigkeit ruhig (1ste Steig. form) (i.e. ruhiger) als am Abend vorher."

"Gross (2te Steig.form) (i.e. groesste) Gas bereitschaft."

Any symbol followed by one of these degrees of comparison must be an adjective, and its occurrence, singly as well as accompanied by the degree of comparison, should be noted, and its function inserted, even where it is as yet impossible to define its exact meaning.

6) Zeitwort. (Verb). This group serves to indicate that a word which is only given as a noun in the code must be translated as a verb. Its use is therefore the converse of "Hauptwort", and it should be treated accordingly.

7)

Gegenwart.	(Present Tense.)
Vergangenheit.	(Past Tense.)
Mittelwort der Vergangenheit.	(Past Participle.)
Zukunft.	(Future.)

These serve to indicate the tense of a verb.
Example.

"Regiment melden (Gegenwart) (i.e. meldet) dass

Fiend in unsere verderen Graeben eindringen

(Mittelwort der Vergangenheit)

(i.e. eingedrungen hat)"

Any occurrence of these tense symbols should be noted and treated in a similar manner to Mehrzahl or 1ste or 2te Steigerungs form as described above.

8) Buchstabier Gruppe. (Spelling begins or ends.)

The use of this symbol has been described above when treating of spelling groups and their solution.

SATZ-ZEICHEN

For the very lucid and stimulating treatment of the various Satz-zeichen used in German Field Wireless Code in the section which follows we are indebted to Lieut. D. MacGregor, whose collaboration has been of very great service to us in clearing up knotty points.

It would be very good practice for the beginner in code work to take the examples he gives, and endeavour to solve them before referring to the key which follows.

"A beginner in code solution is apt to fancy that punctuation marks are a very unimportant branch of his subject. This is quite wrong. They are of paramount importance; and any neglect of them, or any slipshod identification, not only bar the way to many valuable discoveries, to which their accurate identification would have led, but obstructs and obscure the whole work of solution. The mistake, if a fatal one, is still natural."

Given a complete, intelligible sentence, it often matters little if a colon be put for a dash or a stop, comma for brackets, or say an exclamation mark be left out.

But the code solver is not dealing with complete or intelligible sentences. At the start he is dealing with wholly unintelligible sentences, and even after a months' work he is hampered by unknown groups, by Morse errors, manuscript or typescript errors, and nearly every kind of doubt and difficulty which can be conceived. Here it is that the Satz-zeichen play their part.

At the start, thanks to the mechanical unintelligent pedantry of the German, they are themselves, some of them, readily discoverable, and they lead directly to solution of the preliminary difficulties; later, they act as guides to the sense, giving form and construction to the unintelligible, guiding and controlling the conjectures of the investigator.

In a word the study and discovery of these signs is not a mere scholarly refinement, a finishing touch to the work of solution; it is an integral and indispensable part of that work.

The following notes and examples are intended to illustrate this point, and to indicate a few of the technical uses which the solver can make of the Satz-zeichen. But it must not be forgotten that the "rules" given below are not laws of nature or even grammatical canons. "Anforderung" is not always followed by "Doppelpunkt", most often it has no punctuation at all: sentences frequently follow each other without a "Punkt" between them; "8-30" is often written "830". Some codes scarcely punctuate at all. Nevertheless in any code where punctuation is regular it will be found to follow the lines indicated, and a full knowledge of these will be of incalculable value.

I. Punkt.

(a) Separating sentence from sentence; normal and frequent, not infrequently at the end of short, single sentence messages.

(b) As the mark of abbreviation;

"GE-SCH-AE-P-T-S-Z-Punkt"

"ST-RE-ICH-H-Punkt. "

"K-Punkt-T-Punkt-K-Punkt"

"R-Punkt-T-Punkt-R-Punkt"

Note especially GE-XYZ-Punkt, where XYZ should always be tested for FR, giving GE-FR. = Gefreiter.

(c) With figures; very frequent. Between a number and the unit to which it applies:

"An 8 Punkt Infanterie Brigade."

"1 Punkt Kompagnie."

Very frequent is tabulated messages, before and after (more commonly only after) figure or letter headings:

"3 Punkt Anschluss vorhanden 4 Punkt Sicht dunkel 5 Punkt nichts etc.etc."

Rarely = Uhr. "2 Punkt 30" (see under Komma)

Regular in dates: "12 Punkt 1 Punkt 18 Punkt"

(d) After the "address to" and before "address from":

"Brigade Punkt Lage ruhig Punkt Unterschrift K-T-K."

The following pair of actual messages affords an excellent example of various uses of the Punkt and of the incalculable value of the Punkt in the initial stages of solution. On the basis of these messages alone some 15 identifications can be made. The beginner should try his skill on these. The identifications are given below.

```
A)   TL v LQ 0245 GR 12) ufk rur kni ult pwl rur ufo kqt khy rnd
rst uvg

B)   LQ v TL 0245 GR 48) ufk uvg kqt rof kni knw uuo rqw rur rwl
ult kni rur rwl ujq rfp uiw kld kni rzt uzm ujm rwl rtq rxp kni
kwr kvt kni kpg rzt rzi kbd ulg kgd rwl rur rtz ryp ult rbz kni
rzt uzm rur ult rur
```

In passing, a word or two on the "Punkt (nicht das Satz-zeichen)". This is used in the following ways:-

(a) Topographical:

"Zwischen Punkt L and K im Planquadrat" etc.

Frequently preceded by "rot" or "blau".

(b) As a word or part of a word "Zeit-Punkt" "Punkt-lich"

(c) As the "Satz-zeichen". This is naturally very rare, but is commoner than might be supposed and has frequently been exceedingly useful.

In general, Punkt (nicht das Satz-zeichen) is a very valuable group and demands great attention. It must on no account be called "Kartenpunkt" or its other uses will be obscured, and the colour identifications (a very difficult subject, the investigation of which is still in its infancy) to which it often gives the first clues, will be hampered and delayed. "Kartenpunkt" for which there is a separate group is probably very uncommon.

II. Komma.

Less frequent and, on the whole, markedly less useful to the solver than the Punkt.

(a) Normal use – separating parts of a sentence.

(b) With figures = Uhr or decimal point – Very common.

(c) Very rarely for Punkt after an abbreviation.

(d) "KOMMA-N-D-O" used to be frequent, but seems never to be used now.

(e) In tabulated messages occasionally used as follows;-

"3 Punkt vorhanden 4 Punkt dunkel 5 Punkt Komma

6 Punkt unveraendert" etc., where evidently Komma stands for "nichts" or the like (also Bindestrich & Trennungsstrich) or means that 5 and 6 are "unveraendert".

III. Doppelpunkt.

Quite normal in use. The locus classious is after "Anforderung" but it is frequent after any heading;

"Meldung Doppelpunkt" "Eigene Tactigkeit Doppelpunkt" "Vorluste" etc.etc.

Also found in map scales. (See example given under "Klammer") It naturally overlaps sometimes with Trennungsstrich. e.g. "Losungswort : Deinz" and "Losungswort - Deinz" are equally correct.

IV. Bruchstrich.

Not frequent but easy to identify and enormously useful. But it must be identified exactly; under no other name does it smell so sweet. A vague rendering such as Strich or Komma hinders, not helps.

(a) "1/4 Stunde" – not common, but it must not be thought that an example of this use is necessary to prove the identification. The use and value of the Bruchstrich was discovered independently of this simple case; and the identification can now be made and used with absolute confidence in any code without a thought of fractions.

(b) Between Battalion, Company or Battery and Regimental numbers.

"1/116" = Battalion 1 Regiment 116;
"12/94" = 12th Kompagnie Regiment 94 and so forth.

But the usage does not stop here. The following is a pretty "Bruchstrich identification";-

"KGG / Kiel" (presuming that KGG is known not to be a number) = Battalion I II or III Regiment Kiel.)

Or take the following equation (signatures of corresponding Meldungen on successive days):

"RMC/RSJ" = "2/RSJ" – solve for the two unknown RMC & RSJ! Clearly RMC = Battalion II, RSJ = Regiment so & so – the Regimental number is obtained from the order of battle maps.

(Note: the equation RMC XYZ RSJ = 2 XYZ RSJ, is of course, easily soluble for the three unknowns in the same way, so that the previous knowledge of the Bruchstrich was unnecessary here. But this is an exceptionally simple and lucky case and usually one is dependant entirely on the Bruchstrich for this kind of identification. Of course in the later stages of a code the group for Battalion I II & III are quite clearly recognisable on other grounds.

The value of the Bruchstrich, as of the other Satz-zeichen, belongs mainly to the initial stages so far as direct identification is concerned.

(c) In Machinengewehr 08/15.

(d) In the various phrases "Empfang 2/2" "Rier 1/1" etc.

(XYZ 2/2
(Flieger Taetigkeit XYZ rege

where of course XYZ = beiderseits.

(e) Sometimes in map references.

V. Trennungsstrich.

This overlaps with Bindestrich in many uses and until recently was confused with the word "Unterschrift."

(a) Separating "address to" and "address from" from the text. In this use it is seldom (never) preceded by Punkt. "Unterschrift", which is very common, naturally only separates "address from" from the text and may or may not be preceded by Punkt. In Caesar RIW was called Trennungsstrich although this left UUD, a palpable Satz-zeichen, at a loose end. The former was, it is now clear, "Unterschrift".

(b) As a dash or "Gedankenstrich" in sentences its use is quite normal. Sometimes preceded by Punkt.

"Besatzungen gesund Punkt Trennungsstrich Satzbuecher erhalten."

(c) = bis. (cf. Bindestrich.)

(d) See Komma (e). (Trennungsstrich and Bindestrich are much commoner in this connection than Komma.)

VI. Bindestrich.

(a) Normal use as hyphen:

"Artillerie-Schutz-Stellung"

"Funken-Telegraphie Bereitschaft"

"Strasse Messines-Wervicq"

(b) = bis. (cf. Trennungsstrich)

(c) See Komma (e)

(d) With figures, in giving strengths of units, (note position of Punkt – see Punkt (c)

"1 Punkt Kompagnie 2 Bindestrich 5 4 2 Punkt Kompagnie 2 Bindestrich 13 Bindestrich 7 3 3 Punkt Kompagnie, etc.etc."

i.e., No.1 Company, 2 Officers, 8 N.C.O's and 54 men, etc.

A run of numbers in this form may easily yield identifications, such useful words as Kompagnie, M. G. Kompagnie, Minenwerfer, Battalion, and others, which the following example illustrates;-

"uqv ksc kza 12 ksr Bindestrich 32 ruv Bindestrich 292 rzs kjv kza 2 rzs rlc"

Identify ksc kza ksr ruv rzs and, with the help of the following – uqv kjv and rlc;-

"Straufeuer auf den hinteren uqv mehrzahl"

"Sofort dringend ein Wagen fuer ein leicht und 2 rlc."

VII. Fragezeichen.

Frequent and normal in use, but very often omitted where there is no ambiguity. Very occasionally followed by Punkt at the end of a short message. Its importance for the discovery of other groups – ist, sind, was, wie, warum, etc.,– is plain. The following should be tackled. A reasonable conjecture can be - and was - made for the four underlined groups on these messages alone; it proved correct, and was of great use in solution when more material came to hand. (The Fragezeichen is omitted in one of these messages).

Dec. 12th. 69 v ZB Zif 3) rrr kzj ure

" ZB v 69 Zif 9) ure etc.etc.

" " NQ v OY GR 2) ure rkm

" " LQ v GU GR 9) ukt &c. &c. rkm

VIII. Ausrufungszeichen.

Commoner than might be supposed. Comes after commands, urgent and reproachful questions (Wo bleibt Verpflegung! &c) and, of course, "verboten". Not of great help to the solver, but sometimes gives a useful clue since it indicates the general nature of the preceding message. Negatively, its discovery is a great advantage; for it is a thorn in the side so long as it rests unidentified.

IX. Klammer.

Rare and elusive. Is usually given away by a foolish operator using the same group for the beginning and the end of the parenthesis – after that the way is smooth. Generally useful when found; unidentified it is a most treacherous and dangerous will o' the wisp.

(a) Normal – for any parenthesis.

(b) Very rarely enclosing the heading numbers in tabulated messages.

Fill in the blanks in the following:

"Zwischen – – C und D im – 7D 36C – 1 Doppelpunkt 10 – -"

Solutions to examples;-

(a) An K Punkt T Punkt K Punkt mitte bitte morgen Meldung Regiment.

(b) An Regiment mitte eine Punkt maessig (uuo feuer (rqw Kaliber K Punkt T Punkt K Punkt Bindestrich rfp Haus zwei Punkt ohne Aenderung drei Punkt vorhanden vier Punkt dunkel fuenf Punkt Abloesung ohne neu-ig-keit sechs Punkt K-A-L-T sieben Punkt ohne Aenderung K T K.

The identifiable groups are underlined in red, those for which a vague but valuable guess as to their general nature could be made in blue, – e.g KQT of which it can only be said that is say rechts, mitte, links, nord, sud, etc. – a valuable borrowing of the field of search.

It may be objected that UJP might be zwei – it follows a Punkt after K T K. This is quite fair; and the figure identifications should perhaps read ROF eins, UJP ?2, D ?2 or 3 etc. The difficulty however would be cleared up very quickly.

VI. Graben Staerke Doppelpunkt 12 Offizier Bindestrich 32 N/Offizier Bindestrich 292 Mann Verluste Doppelpunkt 2 Mann schwer verwundet.

VII. Wo bleibt Anforderung

Anforderung &c.&c.	These of course are only
Anforderung ?	"reasonable conjectures" not
Ist &c. &c. ?	certain identifications.

IX. Zwischen Rot or Blau Punkt C und B im Planquadrat 7D 36C (1 : 10 tausend)

GENERAL HINTS AND SUGGESTIONS

It cannot be too frequently insisted upon, at this as at every other stage of code solution, that work on back messages should go on concurrently with that on the new material which continues to come to hand.

In fact it is often far more useful to concentrate on a dozen or more back messages, where there are frequently some which contain only a few untranslateable groups, or at any rate, some which have reached a sufficiently advanced stage of progress to enable the general meaning of the whole message to be conjectured.

It is necessary to dig deeply as well as widely in the process of code solution, and one message, if worried as a dog worries a bone, will sometimes yield more marrow than several pages discursively scanned.

It is well never to insert a conjectural translation into the code sheets, until it has been definitely proved. This is a dangerous proceeding and leads either to preventing the right meaning of the group being discovered, or to wrong conjectures being made about the surrounding groups. All theories still in the air should be written on a separate sheet and kept until verified or disproved.

DISTRIBUTION OF WORK

When there are several people working on one code – and the more, not only the merrier, but also very much the faster – it is well to divide the work among them in the following manner.

One should sort all material as explained at the beginning according to place of origin, destination, etc., others should type all messages received in the manner laid down earlier on.

Several copies of each sheet should be made for distribution to those who have to work on them.

All sheets should be clipped together in such a manner that they can be easily handled, and should be kept in consecutive order, so that their subject matter may be chronologically arranged.

Others should be responsible for keeping an up-to-date index of all groups occurring in the code.

One person should be responsible for recording all identifications of code groups in a special index, correcting wrong or insufficiently specified meanings as the right meaning is discovered.

The rest of the available staff should be the actual solvers.

One person should be the controlling mind of the whole work of the code. He should check all theories, be personally responsible for the accuracy of every identification inserted in the index, suggest fruitful lines for experiment, and distribute any possible clues discovered among the remainder of his staff for separate experiment.

When one clue seems likely to be a fruitful one, everybody should work at it until it either proves to be the right one or is definitely discarded as leading nowhere.

All those engaged at work on the same code should work in harmony and conjunction one with the other.

No personal motives, and no jealous desire to keep possible clues from others, in order to have the credit of discovering or proving it, should be allowed to enter into the work.

Every mind should be bent towards the same end, namely the binding of the first identification to start building on, and the complete reduction of the whole code at the earliest possible moment.

Two heads are always better than one, and mutual discussion of possibilities will lead very far on the right road.

Nevertheless after a certain stage has been reached it is often well to divide the work more or less roughly on the following lines. One person might concentrate on initial and final groups, another on an exhaustive study of numbers, another on spelling groups, another on common words and phrases, another on Hilfs-signale, and another on the discovering of the exact function of all the various marks of punctuation.

At the same time, as the code is an entity, it is obviously impossible to lock up these various things in water tight compartments.

The discovery of a group for a particular unit will help in that of numbers, the discovery of a note of interrogation will assist in finding frequent interrogative words, and so on in every aspect of the work.

In conclusion enough has been said to prove that no code ought to be insoluble, given a sufficient quantity of material, a proper method of work, the necessary qualities in the would-be solvers, and sufficient time between the changes of the code-book to admit of the reduction reaching such a stage as to yield information even if only fragmentary.

In code as distinct from cipher a certain length of time must elapse before complete or even partial reduction is possible. The time taken is directly proportionate to the amount of material to work on, to the amount of outside information or of analogy with previous codes available, and to the number and experience of those engaged on it.

In a cipher a fortunate shot may result in the finding of the system, periodicity or keyword on the very first message, or at any rate on two or three, and the key once discovered all material enciphered on the same system is immediately decipherable, whereas with a code, the translation of one message does not render the other messages decipherable.

Cipher deals, moreover, with the more or less mathematical arrangement of 26 letters, while code deals with anything from two to three thousand words.

It is obvious to the meanest intelligence that no meaning can be conjectured for a code group until it has been used in messages at least once, and frequently not until it has been

used sufficiently often to enable its sequences to be experimented upon.

A code is not solved in a day, nor even in a week, not even by a miracle. Complete reduction of a code can only be attained when every group existing in it has been used in messages.

Nevertheless it is often possible, as shown above, to obtain certain amount of very valuable information, even when only about a hundred groups are solved, especially if several of these are the groups for numbers and units.

With the aid of the numbers, dates, times of day, and identifications of units are discoverable.

One final word. The fundamental principles of science and inductive logic hold good in code solution as in any other similar study. The material having come to hand, the phenomena are present.

Observation, experiment, hypothesis, verification are the links in the chain, and when the chain is complete in every link, a certain feeling of gratification may legitimately exist as the result of "something attempted, something done", which may help to shorten the war if only by one day.

APPENDIX 9

We will now give a selection of specimen messages actually intercepted and deciphered within the last twelve months.

These messages will serve a double purpose; firstly of showing the value to be obtained from the labours of the solvers, and secondly of showing the general character and subject matter of the messages sent by German Field Wireless. They will act therefore as a direct incentive to the solver, and as a basis for analogy in solving new codes.

When the key of a cipher was discovered, or when the code had reached a sufficiently advanced stage of solution, these messages were decipherable immediately on interception. In other cases a certain delay was inevitable until the key was discovered. In the majority of the following cases, however, the information contained in the messages was known to us as soon as to the enemy recipient.

The messages numbered consecutively from 13 to 25 are of very great interest. They were all received and deciphered in the course of the great German retirement in the Somme district in March 1917, and give direct indications, not only of the fact of the retirement, but in many cases of the actual places to which various units were ordered to retire.

As the exact location of all the German Wireless Stations was known to us, and also the units to which these stations were attached, the orders to dismantle stations and erect them again at places further back from the line, gave an exact indication of the course of the great retreat.

The following examples are only a few of many hundreds received and deciphered, although obviously not all of them contained information of such direct importance, or of such immediate value.

APPENDIX 3 (Specimen page)

(See figure on following page.)

Serial No. 98 Int.E (c) St. OHER.

Intelligence E (c) Summary of Information. Group. Div. Brig. Regts. Call Signs.

	3N		1mar-2mar-3mar	
	2N	4N	2m-3m-5m	
	8BR	15/16BR	19BR-22BR-23BR	
160	54R	108R	246R-247R-248R	RO' UJ XZ ZF
	187		187-188-189	
180	26R	51R	180-119R-131R	OJ GW O'A SQ WO XO' UQ
185	35	87	61-141-176	FZ KF KN MF O'W IX
190	41	74	18-148-152	CS GK OG RF DF G3
	58	116	106-107-103R	
200	239	239	466-467-468	O'D TU' WN XL ZW FD B9 D7
205	16	30	28-29-68	ON RP VS VX DG GL 5K
210	12R	22R	23R-38R-51R	DK DY FL DP WB
213	36R	69R	54-5R-61R	CL GH QF RJ XD
220	7	14	26-163-393	DX FW O'B RG TP VF WK YT ML
	214	214	50-358-363	
	1BR-2	1BR	1BR-2BR-3BR	
290	Artillery	Stations		A'F DA' IW LX
315	8	16	72-93-163	CQ DW NU O'Q SF VU XK YS QW
320	32	64	102-103-177	EI KB
330	5B	9B	7B-19B-21B	BX OZ HA RS WV ZA' TF ZK
350	4	8	14-49-140	DJ FW LA UC VA' U'N TL
360	38L		77L-78L-79R/85L	AW BH EA' LO NX RZ
	44R	87	205R-206R-208R	
	39	61	126-132-173	
415	6B	11B	6B-10B-13B	DV NY LK UG KZ ZD
445	207	99	209-213-98R	JM ZF A'P CT HS NU QU UB WB
	220	4G	190-55R-99R	
	17	34	75-85-89	
470	5BR	9BR	7BR-10BR-12BR	'ES FN' UT WN XC ZX FK YC
	256	236	457-458-459	
505	24	839	133-139-179	BA' IZ JC XO' TH EU' HJ D7
510	221	1RE	41-60R-1RE	LN TC U'I O'W MU' DY IW G2
515	234	234	451-452-453	AU CN PI IO A'C OH O'2
517	16B	9	11B-14B-21B	BI DA LD UK U'A EN ZW J6
520	20	40	77-79-92	IB JF LE SI FA O'E
525	30	60	GrnFus-Ihr-90R	MH PU QR WE
530	24R	48R	104R-107R-133R	EZ HR IU UY ZG SD
534	16R	31R	20R-30R-68R	EA IQ KH RX UZ U'N V9 W1
537	50R	99R	229R-230R-231R	EG LY N1 O'X SR TW U'X Z9
540	9R	18R	395-6R-19R	CT JW O'A RI UF ZS SJ
543	Artillery	Stations (?)		OW GY NC MD
545	107	213	52R-227R-232R	IK HU RM SU' WU' XH GR V6
550	208	185	25-185-65R	BT ID RC RT UN TJ
570	183	33R	184-418-440R	ET HA OW SW XM
	9BR	17BR	3BE-11BR-14BR	
575	206		339-394-4RE	HQ KH KS XK IG 2J

Intelligence E (c) St. OMER (Signed) O. T. Hitchings Captain, o.i/c.

1) 11/9/17 An Gruppe Thomas. Bage. Feind im Abschnitt E und linker Fluegel Abscnitt eingedrungen. Eigene Artillerie soll in Richtung Pappelschnur zu kurz geschossen haben. A.V.O.

2) 11/2/17 Gruppe. Gegen 6 Uhr macht Infanterie bei Pappelschnur Gegenetoss. Unterstutzfeuer wird noetigenfalls angefordiert. A.V.O.

3) 11/2/17 An Gruppe D. Schuesse in Richtung Pappelschnur liegen noch zu kurz. Um eigene Verluste vorzubeugen musste unbedingt zugelegt werden. nach Aussage eines Infanterieoffiziers. A.V.O.

4) 17/9/17 An 32 Infanterie Division. Von Stosstrupp drei schwarz und vier rot. Fuchrer gesund und am Hein verwundeter Englaender gefangen. Kampf Bataillon 177.

5) 18/2/17 Gruppe Thomas. Stark Truppen Anaammlungen bei Moulinruine. Mit Angriff ist zu rechnen.

6) 18/2/17 Schwytz loest Vaux Wald ab. Schubert.

7) 18/2/17 Regiment Caesar. Wird die Nacht vom 21-22 zwei Bataillon abgeloest.

8) 19/2/17 Abschnitt E. Ist Ablossung des ersten Battaillon 231 durchgefuehrt? Wie gliedert sich das erste Bataillon 230? 99 Reserve Infanterie Brigade.

9) 21/2/17 An Regiment Schaskholz. Sofort Verstaerkung. Sonst Stellung unhaltbar.

10) 21/2/17 Mit allem Garaet um 2 Uhr zum Abmarsch fertig sein. Ich schieke drei Leute. Keinen Klartext geben.

11) 22/2/17 An erste Garde Division. Vorposten Stellung durchlaufend mit Truppen. 5 Machinen Gewehr, 5 Granatwarfer besetzt. Anschluss rechts und links erfolgt erst heute Nacht. Zweite Garde Reserve Division.

12) 10/3/17 8 Uhr 30 vormittags raeumt Regiment Bremen Irles. Die Vorposten der Garde bleiben stehen zur Sicherung unseres Anschlusses. Mit der Garde haben Vorposten zu bleiben. Sicherung den Gefaehrdeton rachten Fluegels hat ohne Verstaerkung der Vorposten stattzufinden. Nicht erforderliche Machinengewehre sind aus den Vorposten herauszuziehen. 2 F Anstellungsbataillon II Ferdinand.

13) 10/3/17 Station setzt sich Morgen 4 Uhr mit vollstaendigen Infanteriegerast nach Moislains in Marsch. Naeheren Befehl. Leutnant Muhlank.

14) 12/3/17 Heller kommt nicht, da Ladestation nach Templeux geht.

15) 13/3/17 Wann kommen unsere Lebensmittel? Wir haben nichts mehr.

16) 14/3/17 Im Laufe der Nacht abbauen. Wagen 6 Uhr dort. Wachtmeister Deter.

17) 14/3/17 Station Schluss. Abholung Morgen frueh. Welp.

18) 15/3/17 V P stuendlich Abbau zu erwarten, laut Befehl von K.T.K.

19) 15/3/17 L D baut morgen ab. Gegen Tragen nochmals versprechen. 7 Uhr 30 Fahrzeug. 9 Uhr Kirchs Equancourt.

20) 16/3/17 Offizier Stellvertreter Remagen. Sofort Armee-Kommando-Funk in Marsch setzen.

21) 17/3/17 Leutnant Hein. Heute Abend abbauen. Auto halb acht Ostausgang Eine-Gouzeaucourt. Leutnant Oullmann.

22) 17/3/17 Station abbaut 12 Uhr. Aufbau Caudry etwa 8 Uhr.

23) 21/3/17 Gestriger Versuch, welcher 4 Uhr wiederholt werden sollte, wird heute 10 Uhr wiederholt.

24) 21/3/17 Morgens Divisionsstab zurueck. 111 Infanterie Division Detachement Bernstorff. Befehl ueber Auflossung vom 203. Marschziel fuer zweite Radfahrer Bataillon I Bellingcourt.

25) 22/3/17 Husaren 14. Ham von Feinde besetzt. Kavallerie der 35ts Infanterie Division geht auf Aubigny und Bray St. Christophe. Gefechtsstelle des Husaren 13 melden 11te Infanterie Division. Selbst Kavallerie 221 Infanterie Division bei Forest. Radfahrer im Kampf mit feindlicher Kavallerie. 11te Infanterie Division weicht auf Etreillers ueber Roupy. Melden wo Anschluss rechts und links. 221 Infanterie Division.

26) 6/5/17 Auf K T K (A) Sofortige Aufklaerung ueber Lage an Brigade. Englaender sollen in Bullecourt sein. Noetigenfalls sofort Gegenstoss. Brigade.

27) 5/6/17 Division Messines. Morgen Meldung. Keine Verbindung mit K T K 6. Ablossung glatt verlaufen. Brigade Messines.

28) 7/6/17 Division. Unterstuetzung dringend erforderlich auf der ganzen Linie.

29) 19/9/17 Die Stellung fuer die neuen Batterien ist auf Strasse Zonnebeke-Droogenbroodhoek.

30) 3/10/17 Es war abgehoert, dass Englaender morgen auf breitem Front angreifen will.

31) 4/10/17 Bataillon 3 Bayr. Res. 5 von Paschendael zum Regiment Nord in Marsch setzen. Rest soll in Bereitschaftsstellung vorgehen. Brigade.

32) 4/10/17 Abschnitt Nord Bayr. Regiment 5 macht Gegenangriff von Paschendael auf Zonnebeke. Eine Bataillon Bayer unter allen Umstaenden ist nach Droogenbroodhoek vorgescheben und stehen zu Gegenstoss zur Verfuegung. Brigade.

33) 21/11/17 Gasangriff nicht 1 Uhr 30 sondern 3 Uhr 30.

34) 22/11/17 Vordere Linie liegt unter Stoerungafeuer. Infanterie arbittet Stoerungsfeuer auf Friedhof.

35) 2/12/17 Sofort melden Lage der eigenen vorderen Linie. Vorfeld ist sofort in alte Linie vorzutreiben.

36) 2/12/17 Vorfeldlinie 895 zurueckgenommen. Hauptwiderstandslinie in unserer Hand. Verlust nicht bekannt. Dringend Munition fuer leicht Maschinengewehr.

37) 11/1/18 Von 8 Uhr 30 bis 11 Gasbereitschaft. Eigener Gasschiessen.

AN EFFICIENT PASSWORD AUTHENTICATION SCHEME BASED ON A UNIT CIRCLE

Horng-Twu Liaw[1] and Chin-Laung Lei[2]

ADDRESS: (1) Department of Information Management, The World College of Journalism and Communications, 116 REPUBLIC OF CHINA and (2) Department of Electrical Engineering, National Taiwan University, Taipei, Taiwan 106 REPUBLIC OF CHINA.

ABSTRACT: In this paper, a password authentication scheme based on a unit circle encoding is proposed. In our scheme, a one-way function and a cryptographic operation such as DES (data encryption standard) are adopted. Besides, in our scheme, the system only need to store a master secret key, and each user can select his own password freely. Instead of storing a password verification table inside the computer system, our method only has to store a corresponding table of identities, which is used by the computer system for validating the submitted passwords. Owing to this scheme the system can quickly and efficiently respond to any log-in attempt, and is suitable for real-time applications. Furthermore, in our scheme, the system does not need to reconstruct any term of the existing key table, when a new user is inserted into the system. Thus, our scheme is suitable for practical implementation.

KEYWORDS: Password, authentication, unit circle, one-way function.

1. INTRODUCTION

Owing to the popularity of computer networks and fast progress of computer technologies on a multi-user system, tremendous information is accessed and shared at any instant of time. However, sharing may cause some undesired phenomena such as unauthorized accesses, inconsistent status of shared resources. Therefore, in a computing environment, the selection of suitable security schemes to prevent the information from being disclosed, copied, altered or destroyed becomes more and more important. Among the existing security schemes, using a password is probably the most widely adopted authentication strategy in log-in procedure because of its inexpensiveness, easy implementation, and user friendliness. To date, many people have devoted themselves to investigating this password authentication scheme [1-2, 4-9]. In general, the computer system assigns each legal user an identity (ID) and each user chooses a password (PW)

for later log-in validation. The most straightforward authentication approach is to store all users' IDs and PWs in a password table as shown in Table 1.

Password Table	
ID_1	PW_1
ID_2	PW_2
⋮	⋮
ID_n	PW_n

Table 1. The password table.

For validating whether the submitted identity ID_i of user i and his associated password PW_i is legal or not during the log-in time, the system will search the password table to obtain the related password PW_i'. If $PW_i' = PW_i$, then user i is a legal user and is permitted to enter the system, otherwise, he is rejected by the system. It is easy to see that the whole scheme depends completely on the security of the password table. Thus, the password authentication system might be destroyed if some information in the password table is altered, or if an intruder can read the system's password table and forge a password to append to the table for later log-in. Thus, if a password authentication scheme is adopted, how to ensure the system's security is an important issue. It is believed that we can ensure the security of the system if the following conditions are satisfied, even if the password table is still in danger.

1. Passwords are stored in their transformed forms rather than in their clear text forms in the password table.
2. An intruder is unable to derive users' passwords, even if he can obtain any information of the password table.
3. Any change or alternation of the password table cannot help an intruder to enter the system.

In order to avoid the security of the system being destroyed, some known password authentication schemes have been proposed [1-2, 4-8]. A one-way function to encode passwords was proposed by Evans *et al* [4]. Lennon *et al* [7]. presented the test pattern scheme to validate passwords. Hwang [5] proposed a password authentication method based on public key encryption. A scheme based on the concept of the quadratic residue algorithm [11] was developed by Laih *et al* [6]. Later, Chang *et al* [1-2] proposed two password authentication schemes based on Rabin's public-key cryptosystem and DES (data encryption system),

respectively. Recently, a password authentication scheme based on Newton's interpolation polynomials was proposed by Lin *et al* [8]. The rest of this paper is organized as follows: In Section 2, some of the existing authentication methods are discussed. An effective password authentication scheme based on a unit circle is proposed in Section 3. Finally, conclusions are given in Section 4.

2. A REVIEW OF SOME PASSWORD AUTHENTICATION SYSTEMS

Using a one-way function to solve the security problem of the password table was first proposed by Evans *et al* [4]. Intuitively, a one-way function is a function that is easy to apply but hard to reverse. Formally, if a function $F : A \rightarrow B$ is a one-way function, it is a one-to-one function and implies that

1. for every x in A, $F(x)$ can be computed easily, and
2. for every $y = F(x)$ in B, it is infeasible to compute x.

Instead of storing the user's password x, the system stores the value $y = F(x)$. Thus, the password table is replaced by a verification table. This verification table is shown in Table 2. When user i tries to submit his identity ID_i with the password PW_i to enter the system for logging-in, the system will utilize the identity ID_i to search the verification table to obtain the relative $F(PW_i')$. If the value obtained from the verification table is equal to the value $F(PW_i)$ computed from the submitted password PW_i with the one-way function F, then user i will be permitted to enter the system, else he will be rejected by the system.

However, this scheme cannot protect against an intruder who might alter information stored in the verification table. Using the existing one-way function F, an intruder might generate a new term $F(x)$ for an arbitrary value x, and then appends $F(x)$ in the verification table, or an intruder might create another one-way function F' and modifies all terms in the verification table in terms of F'. Later, the system would always permit the log-in for the forgery password x and the system's security is then destroyed. In order to prevent this problem of illegitimate entry, a password authentication scheme which makes use of a special test pattern was proposed by Lennon *et al* [7].

Derived from the idea of test patterns, Hwang [5] proposed a password authentication scheme based on a public key encryption approach. One of the weaknesses in the scheme proposed by Hwang is that it needs to store a non-protected table of the test patterns which are generated by the RSA public key encryption/decryption scheme [9]. Besides, owing to the computation of the

RSA cryptosystem, it is not suitable for conventional computer systems. Later, a password authentication scheme based on the concept of public key cryptosystem using quadratic residues [11] was proposed by Laih *et al* [6]. This scheme still has the following disadvantages:

1. The verification table is not protected, thus a legal user has the chance to alter the information in the table.

2. Owing to the application of modular exponential operations during the initialization time, this password generating procedure is very time consuming.

Recently, a password authentication scheme based on Rabin's public key cryptosystem was proposed by Chang *et al* [1]. The method is inspired by Rabin's public key cryptosystem [10]. One weakness of this scheme is that two distinct users may have the same values in their system table. In addition, Chang *et al*.also proposed a simple password authentication scheme based on a conventional cryptosystem DES [3].

A scheme based on Newton's interpolating polynomials (NIPs) is proposed by Lin *et al* [8]. This scheme needs $n/2$ multiplications and $n/2$ additions in average to check the validation of a password, where n is the number of users in the system. When n is large, this scheme becomes impractical. Besides, this scheme needs to store two tables which is more than other methods, in memory.

In the next section, we present an efficient password authentication scheme based on a unit circle encoding. Owing to this scheme thje system can quickly and efficiently respond to any log-in attempt, and is suitable for real-time applications. Furthermore, in our scheme, the system does not need to reconstruct any term of the existing key table, when a new user is inserted into the system. Thus, this scheme is suitable for practical implementation.

3. A PASSWORD AUTHENTICATION SCHEME BASED ON A UNIT CIRCLE

In this section, we introduce the concept of using a unit circle for encoding the password. The main purpose is that points on a unit circle are easy to compute but hard to derive. Given a unit circle C, say $x^2 + y^2 = 1$, in the 2-dimensional plane. Without loss of generality, we assume that there exists a point (x_1, y_1) lying outside C and a directed edge from the circle center $(0, 0)$ to the point (x_1, y_1) is denoted by $\vec{A}$. Thus, a point (x_2, y_2) intersected by C and $\vec{A}$ is located on the circle and can be computed as follows:

$$x_2 = \frac{x_1}{\sqrt{x_1^2 + y_1^2}} \qquad y_2 = \frac{y_1}{\sqrt{x_1^2 + y_1^2}}.$$

Figure 1 illustrates how x_2 and y_2 are assigned by the scheme proposed above.

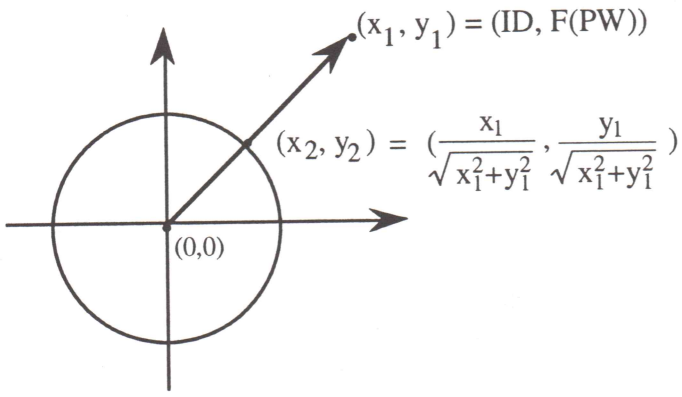


Figure 1. A point (x_2, y_2) is located on the circle.

For a given pair of ID and PW, say ID_i and PW_i, we want to obtain an encrypted form of PW_i. Without loss of generality, let each ID_i be not smaller than 1 and $F(PW_i)$ be the encrypted form of PW_i, where F is a secure one-way function. Furthermore, let $x_1 = ID_i$ and $y_1 = F(PW_i)$. For reducing the truncation error, let the value f_i be equal to the square of x_2 and $t_i = x_1^2 + y_1^2$. Thus,

$$f_i = x_2^2 = \frac{x_1^2}{t_i}. \tag{1}$$

Equation 1 still comes up with a truncation error. For solving this problem, we expand each t_i to b_i, where $b_i = 2\log_2 t_i$. Then f_i is modified by

$$h_i = \frac{x_1^2}{b_i}. \tag{2}$$

Verification Table	
ID_1	$F(PW_1)$
ID_2	$F(PW_2)$
⋮	⋮
ID_n	$F(PW_n)$

Table 2. The verification table.

Furthermore, for avoiding the cooperative attack, we adopt a encryption/ decryption strategy to encrypt h_i based on a conventional cryptosystem-DES. For each key, the system secretly generates a corresponding k_i as follows:

$$k_i = E_{MK}(h_i), \tag{3}$$

where E_{MK} is a encryption function using MK as the key. For later verification, we need to store the k_i's in a table, called the key table, see Table 3.

Key Table	
ID	$k = E_{MK}(h)$
ID_1	k_1
ID_2	k_2
$\vdots$	$\vdots$
ID_n	k_n

Table 3. The key table.

In a typical computing system, each user owns an identity (ID_i) and a password (PW_i) for $i = 1, 2, \ldots, n$, where ID_i is assigned by the system and PW_i is chosen freely by the user.

When user i tries to log-in to the system, he first submits his identity ID_i and password PW_i. The system will utilize the identity ID_i to search the key table for the key value k_i. Then a decryption operation D_{MK} on k_i is performed to obtain h_i, by using the system's master secret key MK as the decryption key, and then evaluate h_i' according to Equation 2. If h_i' is equal to h_i, user i is permitted to enter the system, otherwise he is rejected by the system. Our authentication scheme is shown in Figure 1 and the following example illustrates how this scheme works.

Example 1

Assume that there exists a simple system with four users and MK is a master secret key generated by the system. Let the pair (ID_i, PW_i) be (4, English), (3, French), (6, German) and (2, Chinese), respectively.

Initialization.

Without loss of generality, let F be the one-way function adopted by the system. Besides, let $PW_i s$ be transformed by the one-way function F to 1, 4, 2 and -3, respectively. After executing the Equation 2, we can get all hi's, that is, $h_1 = 0.5$,

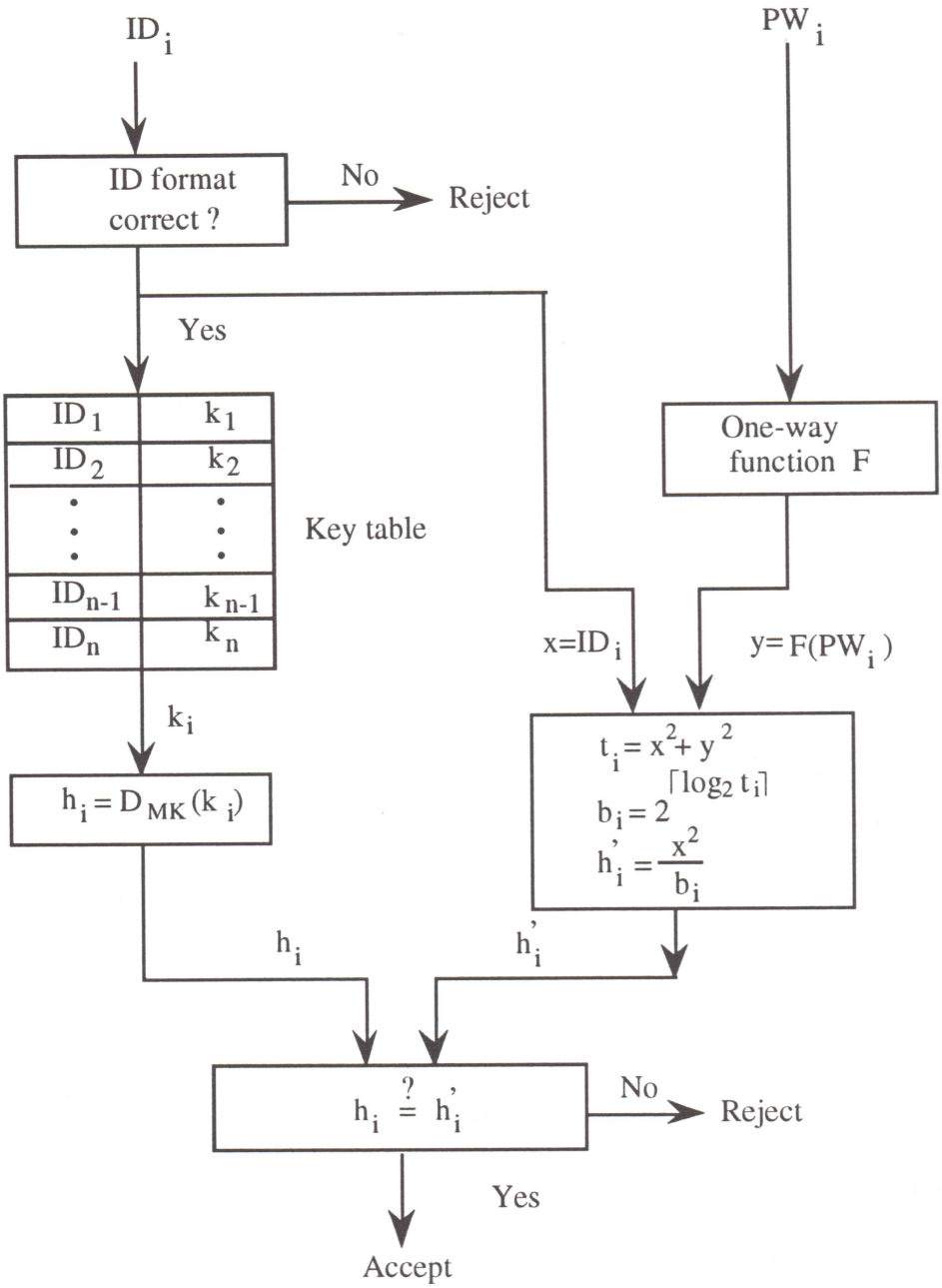


Figure 2. A password authentication scheme based on a unit circle.

$h_2 = 0.28125$, $h_3 = 0.5625$, and $h_4 = 0.25$. Then the system secretly generates a corresponding k_i's according to Equation 3. Without loss of generality, let $k_1 = E_{MK}(h_1) = 0.64$, $k_2 = E_{MK}(h_2) = 2.14$, $k_3 = E_{MK}(h_3) = 62.5$, and $k_4 = E_{MK}(h_4) = -113.24$. For later verification, we store the k_i's in a table, see Table 4.

ID	k
4	0.64
3	2.14
6	62.5
8	-113.24

Table 4. The key table.

Authentication.

If a user submits his $(ID_1, PW_1) = (4, \text{English})$ and tries to log-in the system, his password is transformed to 1 by the one-way function F at once. After searching the Table 4, the key value $k_1 = 0.64$ is found. Then a decryption operation D_{MK} on k_1 is performed to obtain h_1, by using the system's master secret key MK as the decryption key. Furthermore, evaluating the Equation 2, we find that $h_1' = 0.5 = h_1$. Therefore, the user is a legal user and is permitted to enter the system.

Insertion.

Assume that a new user with $(ID_5, PW_5) = (1, \text{Netherlands})$ is inserted to the system and let $F(PW_5) = 5$. A new value $h_5 = 0.03125$ is calculated according to Equation 2 and the system secretly generates a corresponding k_5 according to Equation 3 and then appended to the fifth row of the key table without altering the existing key values k_is. From the above analysis, we find that our proposed password authentication scheme has the following advantages:

1. In our scheme, an intruder could not forge any message of the key table for later log-in, while in the pure one-way function scheme proposed by Evans *et al* [4], an intruder might generate a new term $F(x)$ for an arbitrary value x, and then appends F(x) in the verification table. Later, the system would always permit the log-in for the forgery password x and the system's security is then destroyed.

2. The user can freely choose his own password, while in the authentication scheme proposed by Laih *et al* [6], the user can no right to choose his own password.

3. A new user can be easily added to the system without reconstructing all terms of the existing key table and the generation of a new key value is simple and quick, while in the authentication scheme proposed by Lin *et al* [8], it needs $O(n)$ operation time to generate the new value of their system table.

4. If one user changes his password or a user is deleted, our key table only needs minor adjustment or no change, while in the authentication scheme proposed by Lin *et al.*, the whole system table (called the α-table) needs to be reconstructed.

5. The exposure of key table does not spoil our system.

6. The key table entry is also a function of the ID_i and thus users choosing the same password will have different key table entries. This means that even if one of these passwords were compromised for a given user ID_i, analysis of the key table alone would not reveal other users who have chosen the same password.

4. CONCLUSIONS

Password authentication is the most straightforward authentication scheme of information security. In this paper, we propose an efficient password authentication scheme based on a unit circle encoding. The most significant advantage of our proposed scheme is "simple." Besides, our scheme does not need to store any password verification table in memory, and a user can freely choose his password, which some past password authentication schemes prevented. Furthermore, no modification of the existing values in the key table is needed when a new user is inserted into the system, or an old user is deleted from the system, while almost all past password authentication schemes need. Therefore, we believe that our proposed scheme is easy, simpler, flexible, elegant and practical for real implementation.

ACKNOWLEDGEMENTS

The Authors would like to thank the referees for their valuable comments and suggestions.

REFERENCES

1. Chang, C. C. and L. H. Wu. 1990. A Password Authentication Scheme Based Upon Rabin's Public-Key Cryptosystem. *Proceedings of the 1990 International Conference of Systems Management, Hong Kong.* 425-429.

2. Chang, C. C. and L. H. Wu. 1990. A New Password Authentication Scheme. *Journal of Information Science and Engineering.* 139-147.

3. Denning, D. E. R. 1982. *Cryptography and Data Security.* Reading MA: Addison-Wesley.

4. Evans, A., Jr., W. Kantrowitz, and E. Weiss. 1974. A User Authentication System Not Requiring Secrecy in the Computer. *Communications of the ACM.* 17: 437-442.

5. Hwang, T. Y. 1983. Password Authentication Using Public-Key Encryption. *International Carnahan Conference of Security Technology.* Zurich SWITZERLAND. 4-6.

6. Laih, C. S., L. Harn, and D. Huang. 1988. Password Authentication Using Quadratic Residues. *Proceedings of the 1988 International Computer Symposium, Taipei, Taiwan, R. O. C.* 1484-1489.

7. Lennon, R. E., S. M. Matyas, and C. H. Meyer. 1981. Cryptographic Authentication of Time-Invariant Quantities. *IEEE Transaction on Communications.* 29(6): 773-777.

8. Lin, C. H., C. C. Chang, T. C. Wu, and R. C. T. Lee. 1991. Password Authentication Using Newton's Interpolating Polynomials. *Information Systems.* 16(1): 97-102 .

9. Piller, E. 1988. Survey of Password. *Proceedings of the 1988 International Computer Symposium, Taipei, Taiwan, R. O. C.* 1478-1483.

10. Rabin, M. O. 1979. *Digitalized Signatures and Public-Key Functions as Intractable as Factorization.* Technical Report, MIT/LCS/ TR-212 MIT.

11. Rivest, R. L., A. Shamir and L. Adleman. 1978. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Communications of the ACM.* 21(2): 120-126.

BIOGRAPHICAL SKETCHES

Horng-Twu Liaw was born in Taichung, Taiwan in 1964. He received the BS degree in Computer Engineering from National Chiao Tung University, Hsinchu, Taiwan, in 1986, the MS degree in Applied Mathematics from National Chung Hsing University, Taichung, Taiwan, in 1989, and the PhD degree in Electrical

Engineering from National Taiwan University, Taipei, Taiwan, in 1992, respectively. He is currently an associate professor of the Department of Information Management at The World College of Journalism and Communications, Taipei, Taiwan. He is also the Director of the Computer Center at the college. His research interests include information security, algorithms design, and analysis.

Chin-Luang Lei was born in Taipei, Taiwan in 1958. He received his BS degree in electrical engineering from National Taiwan University in 1980 and his PhD degree in computer science from the University of Texas in 1986. From 1986 to 1988 he was an assistant professor of computer and information science at The Ohio State University. Since 1988, he has been an associate professor of electrical engineering at the National Taiwan University. His current research interests include parallel and distributed processing, operating system design, formal semantics of concurrent programs, design and analysis of algorithms, and information security. Dr. Lei is a member of the Institute of Electrical and information Security, the Institute of Electrical and Electronic Engineers, and the Association for Computing Machinery.

REVIEWS AND THINGS CRYPTOLOGIC

Louis Kruh

ADDRESS: 17 Alfred Road West, Merrick NY 11566 USA.

NETWORK SECURITY

Stallings, William. *Network and Internetwork Security: Principles and Practice*. Prentice-Hall, Inc., Englewood Cliffs NJ 07632 USA. 1995. 462 pp. $55.00.

This excellent book is divided into two sections. The first part, with five chapters, provides a survey of the principles of network security.

Encryption discusses the Convention Encryption Model, Classical Encryption Techniques, Data Encryption Standard (DES), and Triple DES.

Confidentiality Using Conventional Encryption covers Placement of Encryption Function, Traffic Confidentiality, Key Distribution, and Random Number Generation.

Public Key Cryptography describes Principles of Public-Key Cryptosystems, RSA Algorithm, and Key Management.

Authentication and Digital Signatures reviews Authentication Requirements, Authentication Functions, Cryptographic Checksums, Hash Functions, Digital Signatures, and Authentication Protocols.

Intruders, Viruses, and Worms covers each of these subjects plus Trusted Systems.

Part II, with four chapters, is devoted to network security practices with algorithms and applications that are already in widespread use or likely to achieve that status in the near future.

Cryptographic Algorithms describes The MDS Message Digest Algorithm, Secure Hash Algorithm (SHA), International Data Encryption Algorithm (IDEA), SKIPJACK, and LUC Public-Key Encryption.

Authentication and Key Exchange includes Kerboros, X.509 Directory Authentication Service, Diffie-Hellman Key Exchange, and Digital Signature Standard.

Electronic Mail Security discusses Pretty Good Privacy (PGP) and Privacy Enhanced Mail (PEM).

Network Management Security reviews Basic Concepts of Simple Network Management Protocol (SNMP), SNMPv1 Community Facility, and SNMPv2 Facility.

This comprehensive volume is designed for both students and professionals in data processing and data communications. It is clearly written with numerous appendices throughout the book to insure understanding of concepts, algorithms, techniques and other topics. With an extensive glossary, bibliography, list of frequently used acronyms, end-of-chapter problems and suggestions for further reading, this outstanding book serves as a tutorial and handy reference volume.

CHAOS ON INFORMATION SUPERHIGHWAY

Schwartau, Winn. *Information Warfare: Chaos on the Electronic Superhighway*. Thunder's Mouth Press, 632 Broadway, 7th Floor, New York NY 10012 USA. 1994. 432 pp. $22.95.

With more than 125 million computers tying the country together, a major portion of our $6 trillion economy depends on their reliable operation. Information warfare currently costs the United States an estimated $100 to $300 billion per year through HERF (high energy radio frequency) guns and EMP/T (ElectroMagnetic Pulse Transformer) bombs, industrial espionage, hackers, viruses, data eavesdropping, codebreaking, attacks on personal privacy and other means.

Schwartau examines the enormous potential for individual and international espionage, revealing various ways by which one could disable systems, steal or transfer information or money, and alter information in any data bank that does not have sufficient protection.

In his chapter, "Sniffers and the Switch," Schwartau describes how a passive network sniffer, which also contains a small radio transmitter, can be surreptitiously attached to a company's computer network wiring. The radio broadcasts all data and passwords the network processes to a remote receiver.

"The World of Mr. van Eck" examines electromagnetic eavesdropping. Equipment such as computers, printers, fax machines, and video monitors are also electrical devices that conduct current and emit magnetic fields. These magnetic fields can be picked up by a special receiver and read invisibly, passively, and with little fear of detection. In 1985, a Dutch scientist published a paper on the subject containing sufficient details to cause the National Security Agency to classify it. NSA's Tempest specifications eliminates electromagnetic radiation.

A chapter on cryptography ranges from World War II Enigma decrypting to the Data Encryption Standard (DES) and the current Clipper Chip controversy. Schwartau points out that export controls result in "American-designed, public domain DES being manufactured all over the world" while American firms find it almost impossible to sell encryption products outside of the U.S. and Canada. Schwartau claims that NSA "has had its own DES cracking machines for years" and "The Harris Corporation built a system for the government that can crack DES in less than fifteen minutes."

After outlining almost every kind of informational disaster imaginable, the author details current trends in information warfare and calls for a National Information Policy, a constitution for cyberspace and an Electronic Bill of Rights.

ATTACKING DES

Coppersmith, Don. "The Data Encryption Standard (DES) and its strength against attacks." *IBM Journal of Research and Development*, Armonk NY 10504 USA. Vol. 38, No. 3, May 1994, pp. 243-250. Subscription, $74.50 annually (six issues); single copy, $15.00.

In recent years, a new cryptanalytic attack known as "differential cryptanalysis" has been used in an effort to break the Data Encryption Standard (DES). Although the technique seems promising it has not been successful against the full 16-round DES.

DES was developed by IBM with technical advice from the National Security Agency (NSA) and it was adopted as a national standard in 1977. But, though DES' entire algorithm was published in the Federal Register, its design considerations were not disclosed. As a result, many people have speculated that NSA was responsible for withholding design considerations because DES contains a "trap door" or hidden weakness.

Coppersmith, who was a member of the IBM team that developed DES, reveals they were aware of the technique of differential cryptanalysis and built safeguards against it. He maintains that design considerations were not published because it would expose a powerful technique, useful against many ciphers, which had not been mentioned in open literature. The concern was that its disclosure would reduce the U.S.' competitive advantage over other countries in the field of cryptology.

Coppersmith describes DES and differential cryptanalysis. He says the IBM team's awareness of the need to strengthen DES against attacks using differential cryptanalysis played an important role in the design of DES S-boxes and

permutation. He also reveals the design criteria and discusses the role they play in resisting a differential cryptanalysis attack.

FINITE FIELDS IN CRYPTO

Lidl, Rudolph and Harald Niederreiter. *Introduction to finite fields and their applications*. Revised Edition. Cambridge University Press, 40 West 20 Street, New York NY 10011-4211 USA. 1994. 416 pp. $47.95.

The theory of finite fields, a branch of modern algebra, has become important in recent years because of its diverse applications in such areas as combinatorics, coding theory, pseudorandom number generation, and cryptology.

This book, first published in 1986, has been out-of-print but continuing demand has prompted reprinting with some revisions by the authors.

It is designed as a textbook and a background in linear algebra is a prerequisite. Prior exposure to abstract algebra is also helpful although all the necessary information is summarized in Chapter 1. The first part of the book introduces the theory of finite fields with emphasis on those aspects relevant for application. The second part discusses the most important applications of finite fields, particularly to information theory, algebraic coding theory and cryptology.

The chapter on cryptology explores the use of discrete exponentiation in finite fields. Examination of these cipher systems from a cryptanalyst's viewpoint leads to a study of the inverse function, i.e., the index or discrete logarithm in finite fields, and an analysis of its computational complexity. Applications of discrete exponentiation and discrete logarithms are described and several algorithms for the calculations of discrete logarithms are presented. A cryptosystem based on Groppa codes and another on polynomial interpolation in finite fields are also discussed.

Each chapter includes worked examples, numerous exercises, and historical and bibliographical notes.

FILS IS NOW WIR

Cline, Marjorie W., ed. *World Intelligence Review*, Heldref Publications, 1319 18th St. NW, Washington DC 20036-1802 USA. Published bimonthly. Annual subscription: $35.00 for individuals, $50.00 for institutions.

World Intelligence Review (WIR), a new name for *Foreign Intelligence Literary Scene* (FILS), which was founded in 1982, is being published by Heldref

Publications in cooperation with the National Intelligence Study Center.

Bruce Fein, a columnist and attorney, is Executive Editor and will provide a regular editorial as a new feature. Foreign editors knowledgeable in intelligence matters will supply additional editorial leadership. Nigel West, who lives in England and is a prominent author of books on intelligence, has agreed to serve as European Editor.

WIR will continue worldwide reporting and analyzing of intelligence literature and developments in the field, informative articles, book reviews, and "Periodicals and Documents," a valuable listing of intelligence related articles by region.

Subscribers include intelligence officers, teachers, students of foreign affairs and other individuals interested in the intelligence profession and its role in national security.

COMPUTER SECURITY TECHNOLOGY

Amoroso, Edward. *Fundamentals of Computer Security Technology*. P T R Prentice Hall, Englewood Cliffs NJ 07632 USA. 1994. 404 pp. $48.00.

This book is based on a series of tutorial essays designed to help students understand lecture material the author uses in a graduate course on computer security. Assisted by comments of students and colleagues and refined over a period of several semesters the tutorials have been transformed into a text that can be read without great technical difficulty. The author does suggest that a technical background is helpful in some areas.

Each of the 29 chapters provides a clear overview of its topics and covers essential points with examples, ending with a summary, exercises and a complete set of references to more detailed information.

The text can be divided into four basic parts: Part 1 consists of the first five chapters, which discuss Threats to Computer Organizations, Threat Trees, Categorization of Attacks, Trojan Horses and Viruses, and Common Attack Methods.

Part 2, Chapters 6-14, supplies the basic security modeling concepts, which are needed to understand this vital aspect of computer security. Various components of security models are presented and the most familiar ones are described.

Part 3, Chapters 15-26, offers an overview of safeguard and countermeasure approaches for computer security. Amoroso suggests that each chapter provides "an additional 'weapon' to use in thwarting the attacker." These techniques include Identification and Authentication, Passwords, Encryption, Key Management Protocols, Covert Channels, and others.

Part 4, Chapters 27-29, cover three giant topics, Network Security, Database

Security, and Evaluating Security, which are application-oriented and rely on material reviewed in earlier chapters.

Anyone with an interest in computer security should find something of value in this comprehensive volume. The author has compiled an extensive annotated bibliography of more than 250 papers, reports and texts dealing with computer security, which is a thorough guide to the more detailed security literature. Readers seeking the best references in the field can refer to the author's list of "Twenty-Five Greatest Works in Computer Security."

FUNDS NEEDED FOR BLETCHLEY PARK MUSEUM

The Bletchley Park Trust was formed in 1992 to preserve Bletchley Park and keep its buildings from being demolished. The aim of the Trust is to acquire the site and develop museums of cryptology and the history of computing in renovated and refurbished buildings. The museum complex would recognize the extraordinary accomplishments that took place there between 1939-1945, particularly in relation to the breaking of enemy ciphers.

In addition to seeking donations, the Bletchley Park Trust offers the following items for purchase. (Please note that prices are in British pounds/pence.)

Please make ALL cheques payable to Bletchley Park Company Ltd.

Prices in Pounds Sterling and Pence - plus 50 for p&p for 1 item
or £1-00 for three items or more

Code Breakers (by F. H. Hinsley and Alan Strip)	17-95 + 2-00 p&p
Reproduction Battle Plan maps	3-50 p
Postcards (Mansion Bletchley Park)	25 p
New Items For Sale Bletchley Park ball point pens* (black and gold)	2-50 p
Bletchley Park: Britain's Best Kept Secret Ultra's Base at Bletchley Park	6-99 p (Trust's first book)
Local Bletchley Newspaper (1944)	50 p
Special Bletchley Park 'D' Day Commemoration First Day Cover Stamps & Coins	4-95 p
'D'Day Commemoration First Day Cover Stamp Only	3-95 p
Coins issues 2nd World War (in picture frame)	4-95 p

* Please allow 28 days for delivery.

In addition ALL items previously offered for sale can still be obtained.

All proceeds go to support the work of The Bletchley Park Trust

In late 1993, the Trust moved into the "Bungalow" within Bletchley Park. Since February 1994, an exhibition has been open to the public every other weekend. Enigma, Lorenz, and Geheimschreiber machines are on display along

with artifacts based on Bletchley's other wartime activities. The Computer Conservation Society is developing a display and hopes to rebuild Colossus Mk. 1 in 'H' Block shortly.

Funds are need to purchase the property and develop the museums. Donations can be sent to Bletchley Park Trust Ltd., The Bungalow, Stable Yard, Bletchley Park, Milton Keyes MK3 6EF, United Kingdom.

SECRET MUSICAL CODEWORDS

Caxton C. Foster

ADDRESS: P. O. Box 488, E. Orleans MA 02643 USA.

ABSTRACT: We offer musical a sign - counter sign example and ask readers if they have ever seen any others.

KEYWORDS: Musical codewords, whistled codewords.

Many groups use signs and counter signs for recognition. Little children playing "exclusive club" often make up elaborate schemes for distinguishing members (who of course, they know perfectly well!) from non-members.

My stepfather, Thomas Churchill Langhorne, was a member of such a club when he was a boy. Another member of the same club was named Ole Speaks. Mr. Speaks (1874-1948) became a well known song writer and singer. Among other songs, he composed the music for "Sylvia" and "The Road to Mandalay." So it will not come as a great surprise to discover that the recognition signals used by this club were two musical phrases. As far as I know, this use of whistled tunes is unique. I would be most interested to find out if other readers are aware of similar cases.

The exclusive club sign and countersign are offered below:

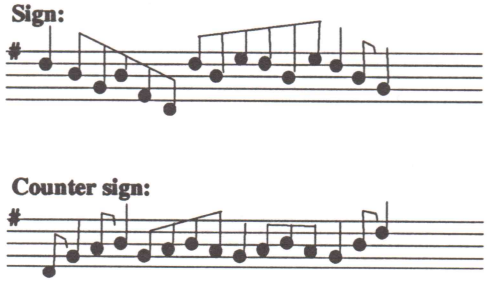


Figure 1. Sign and counter sign.

SUBSCRIPTION INFORMATION

CRYPTOLOGIA is a quarterly journal with issue dates of January, April, July and October. The four journals issued each year constitute one volume. The January 1995 issue is Volume XIX, Number 1.

Subscription prices (US dollars): $40.00 per year for US, $44.00 per year for non-US. A subscription begins with the current issue as of date of receipt of request unless otherwise instructed. Most back issues from January 1979, Volume 3, Number 1 to current issue are available from the Editorial Offices for $11.00 in US and $11.00 non-US. Specify volume, number and issue date when ordering. Write for prospectus giving table of contents for all issues.

All orders, checks and inquiries should be sent to: **CRYPTOLOGIA**, Rose-Hulman Institute of Technology, Terre Haute, Indiana 47803, USA. Make subscription checks payable to **CRYPTOLOGIA**.

Note to subscribers: The number in the upper right corner of your address label indicates the last issue of your subscription. The right hand (single) digit indicates the Number and the remaining left hand digits indicates the Volume of the last issue in your subscription. Renew or extend your subscription now.

CALL FOR PAPERS

CRYPTOLOGIA welcomes articles on all aspects of cryptology. We especially seek articles concerning mathematics and computer related aspects of cryptology. Articles describing new cryptosystems and methods of cryptanalysis of cryptosystems, historical articles, memoirs and translations are all sought.

Send mathematical and computer related papers to Brian J. Winkel, Division of Mathematics, Rose-Hulman Institute of Technology, Terre Haute IN 47803 USA.

Send papers, inquiries and letters concerning cryptographic machines, devices, and equipment to Louis Kruh, 17 Alfred Road West, Merrick NY 11566 USA.

Send historical and other non-technical articles to David Kahn, 120 Wooleys Lane, Great Neck NY 11023 USA.

Any paper may also be sent to the Editorial Office, **CRYPTOLOGIA**, Rose-Hulman Institute of Technology, Terre Haute IN 47803 USA.

Three copies should be submitted and one should be kept by the author as a protection against loss. Manuscripts should be legibly typewritten, or reproduced from typewritten or computer printer copy and double-spaced with wide margins. All papers should have an Abstract and a Keyword list after the title and author. In addition there should be a short, paragraph form, biographical sketch of the author(s) at the end of the paper. Editorial style follows the University of Chicago Press *Manual of Style*. Please adhere to the footnoting style found in **CRYPTOLOGIA** articles. Diagrams should be done in black, suitable for off-set photo reproduction, and clearly labeled with a legend. Photographs should be clear and glossy. Indicate whether or not the photo print enclosed is to be returned.

While the ultimate responsibility for the accuracy of the material presented lies with the author(s), the Editorial Office will do its best, through the refereeing and the consultation process, to help insure correctness.

Authors will receive fifty reprints of their article and two copies of the issue in which their article appears.

CRYPTOLOGIA

A Quarterly Journal Devoted to Cryptology
Volume XIX Number 2 April 1995

Table of Contents

Published Quarterly at Rose-Hulman Institute of Technology
Terre Haute Indiana 47803 USA